Sri Lanka Institute of Information technology
2024
Web Security - IE2062

Year 2, Semester 2

Web Security Assignment

http://dyson.com/

IT22572974
I.W.A.R. DUSHMANTHA
Y2.S2.WD.CS.01.02
MALABE CAMPUS

Table of Contents

01. Acknowledgement

02. Assignment objectives

03. Methodology

04. OWASP

05. Severity levels of security issues

06. Assignment scope

07. Dyson

7.1. In scope domains

7.2. Out scope domains

08. Bug Bounty Reports

I. Report 01

Target main domain : http://dyson.com/

Information Gathering

- Whois.com
- Sublist3r
- Recon -ng Tool
- Crt.sh

Alive sub domains

- Httprobe

Find Archived information

- Wayback machine
- Wayback URLs

DNS Enumeration

- DNSrecon

Public Device Enumeration

- Censys
- Shodan

File system structure

- Dirb Tool
- Dirsearch

Firewall protection against target domains

- Wafw00f

Vulnerability Analyzing Phrase

- Nikto
- Wapiti
- Whatweb
- Netsparker

II.Report 02

Target sub domain : **Webmail-SG.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

III.Report 03

Target sub domain : **adminqaservice.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

IV.Report 04

Target sub domain : **api-alexa-login.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

V.Report 05

Target sub domain : **http://www.careers.dyson.com/**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

VI. Report 06

Target sub domain : **api.cp.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

VII. Report 07

Target sub domain : **api.cpstage.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

VIII. Report 08

Target sub domain : **demo3D.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

IX.Report 09

Target sub domain : **admin.shop.kr.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

X.Report 10

Target sub domain : **staging.admin.shop.kr.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

XI.Report 11

Target sub domain : **privacy.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

XII.Report 12

Target sub domain : **teamcenterMY.dyson.com**

Vulnerability Analyzing Phrase & Recommendation

- Nikto
- Wapiti
- Whatweb
- Netsparker

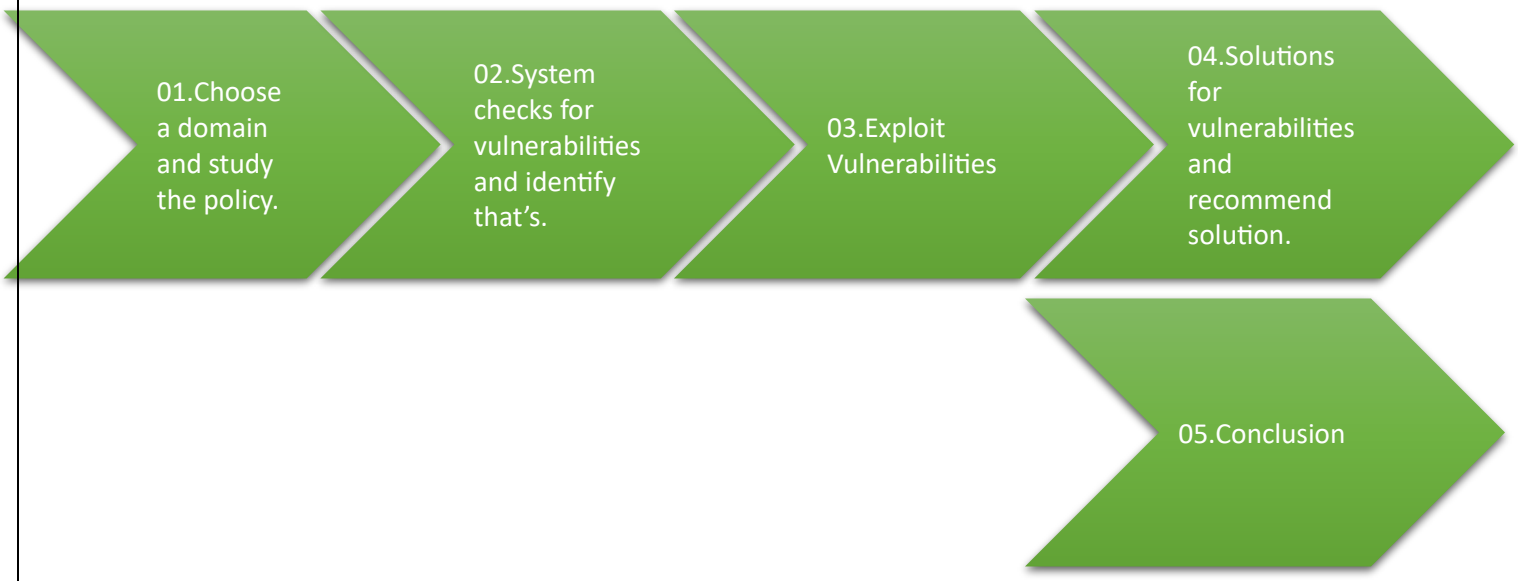
1. Acknowledgement

Bug bounty programs play an important role in improving firms' security posture by leveraging the capabilities of ethical hackers to uncover and patch vulnerabilities in online platforms. As such, I am grateful to the different firms around the world who have launched bug bounty programs allowing ethical hackers to contribute to the security of digital ecosystems. The expansion of bug bounty programs provides ethical hackers with various opportunities to demonstrate their skills and experience ultimately encouraging a safer online environment. This study focuses on the value of bug bounty programs and presents insights that help to continuing efforts to improve cybersecurity

2. Assignment Objectives

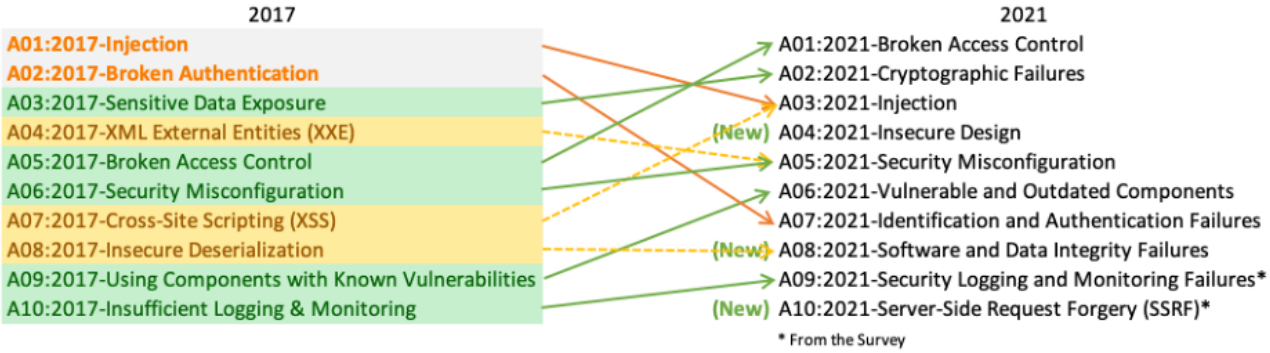
The security assessment of the http://dyson.com for the second year second semester Web Security Module. The purpose of this assessment is to discover the vulnerabilities in the target domain and to indicate the subsequent risk level for the vulnerabilities.

3. Methodology



4. OWASP

The Open online Application Security Project (OWASP) has determined the top ten most significant threats to online application security. Successful Bug Bounty hunting requires an understanding of these dangers and taking steps to mitigate them.



1. Broken Access Control

- In this instance, access limitation and authentication are taken into account. Attackers may obtain privileged user settings or sensitive data if these functionalities are made susceptible.

- Insecure access control methods and configuration problems are hard to find since automated processes can't always check for them. Penetration testing can find authentication gaps, but other techniques are needed to find configuration problems.

- Weak access controls and issues with credential management can be avoided with the use of secure coding techniques as well as proactive steps like shutting down administrative accounts and controls and using multi-factor authentication.

2. Cryptographic Failures

- This was referred to as exposure to sensitive data.
- This renewal has brought attention to cryptography's vulnerabilities which could expose private information or compromise systems.

3. Injection

- Injection attacks include SQL injections, command injections, CRLF injections, and LDAP injections, among others.
- By taking advantage of the code, in injection attackers insert their own code into the program. The attacker will be regarded as a trusted user because the program is unable to identify the problem.
- The latest edition of OWASP states that injection includes cross-site scripting.

4. Insecure Design

- The discovery of this new category occurred in 2021.
- Design flows are the primary focus of this risk.

5. Security Misconfiguration

- Sensitive data can be easily accessed with a significant risk of assault.
- The former category known as XML External Entities (XXE) is now included in security misconfiguration.

6. Vulnerable and outdated Components

- Previously identified as utilizing known vulnerabilities and components.
- Risk assessment and testing was challenging.

7. Identification and Authentication Failures

- once known as compromised authentication.
- Improper implementation of session management and authentication calls can be a major security issue.
- Attackers could be able to easily take over the identities of genuine users if they find these vulnerabilities.
- One way to stop authentication errors is to use multifactor authentication. Run DAST and SCA scans prior to code deployment in order to identify and resolve implementation error problems.

8. Software and Data Integrity Failures

- This category is also brand-new.
- This emphasis on assuming things without checking their integrity—software updates, important data, and CI/CD workflows.

9. Security logging and monitoring failures

- Inadequate monitoring methods and the failure to record attacks or failures could contribute a human element to security problems.
- Threat actors use delayed remediation timelines and inadequate monitoring to initiate attacks before you have a chance to detect or react.

- Make sure that all login, access control, and server-side input validation errors are recorded with context so that suspicious activity may be recognized in order to prevent issues brought on by inadequate logging and monitoring.

- Another great method for determining whether parts of your application don't log enough is penetration testing. Establishing suitable monitoring protocols is also essential.

10. Server side request forgery

- A low incidence rate, above-average testing coverage, and above-average ratings for potential to exploit and impact are all indicated by the data.

- This category includes situations where experts in the field of security inform us about important information that isn't already included in the data.

5. Severity levels of security issues

There are four risk levels can be identified in vulnerability scans. They are,

1. Critical
2. High
3. Medium
4. Low

1. Critical Level

- At this stage, an attacker has the ability to access sensitive data or run code on the application server or web application.

- Some examples of critical level vulnerabilities are SQL Injection, Remote Code Execution, and Command Injections. Attackers can carry out destructive actions, such as compromising the confidentiality and security of an online application or affecting its availability, by taking advantage of this kind of vulnerability.

- Resolving these issues is crucial since automated exploitation techniques are widely available and used.

- Since the web application is susceptible and can be attacked at any time, these levels of vulnerabilities need to be repaired right now.

2. **High Level**

- An attacker can take advantage of this level to steal sensitive or session data from the server or application.

- This level differs from the critical level since an attacker at this level cannot run a code or a command in the server or application.

- Should an XSS vulnerability be found, the attacker may be able to If an XSS vulnerability is found, an attacker may be able to take control of the user's cookies or run script code in their browser.

- If the XXE vulnerability is found, the attacker can access the server's sensitive data and request resources from both internal and external sources.

3. **Medium Level**

- At this stage, most application setup problems allow attackers to steal confidential data from the server.

- Additionally, the attacker needs to be more skilled in order to take advantage of these level vulnerabilities. that to take advantage of essential and high levels.

- To exploit these kinds of vulnerabilities, it could be necessary for certain special conditions to exist. For instance, an attacker needs to be in a position where they can listen in on the victim's connection in the event of SSL/TLS certificate issues or TLS misconfiguration.

- Even if, unlike Critical and High Severities, exploiting Medium Severity vulnerabilities necessitates peculiar circumstances and does not directly affect the program or system, they should nevertheless be fixed to ensure the security and legal compliance of your web application.

4. Low level

- Low level security includes setup mistakes, information leakage, and the absence of some security mechanisms. However, problems at this level can mix with those at higher levels, and using social engineering to manipulate others can seriously jeopardize the application.

- Furthermore an attacker can check the vulnerability database to determine whether a web application version is exploitable or not when it discloses its version number.

- For instance Netsparker has discovered vulnerabilities pertaining to username disclosure in the Linux and Windows operating systems. An attacker may be able to take advantage of them as soon as they are flagged.

- In addition, the x-frame-option header error configuration governs whether a website loads via its own means, through another website, or neither. If there is a problem with the x frame option header, the attacker can utilize this to deceive a legitimate user into clicking on a malicious link so they can take advantage of it.

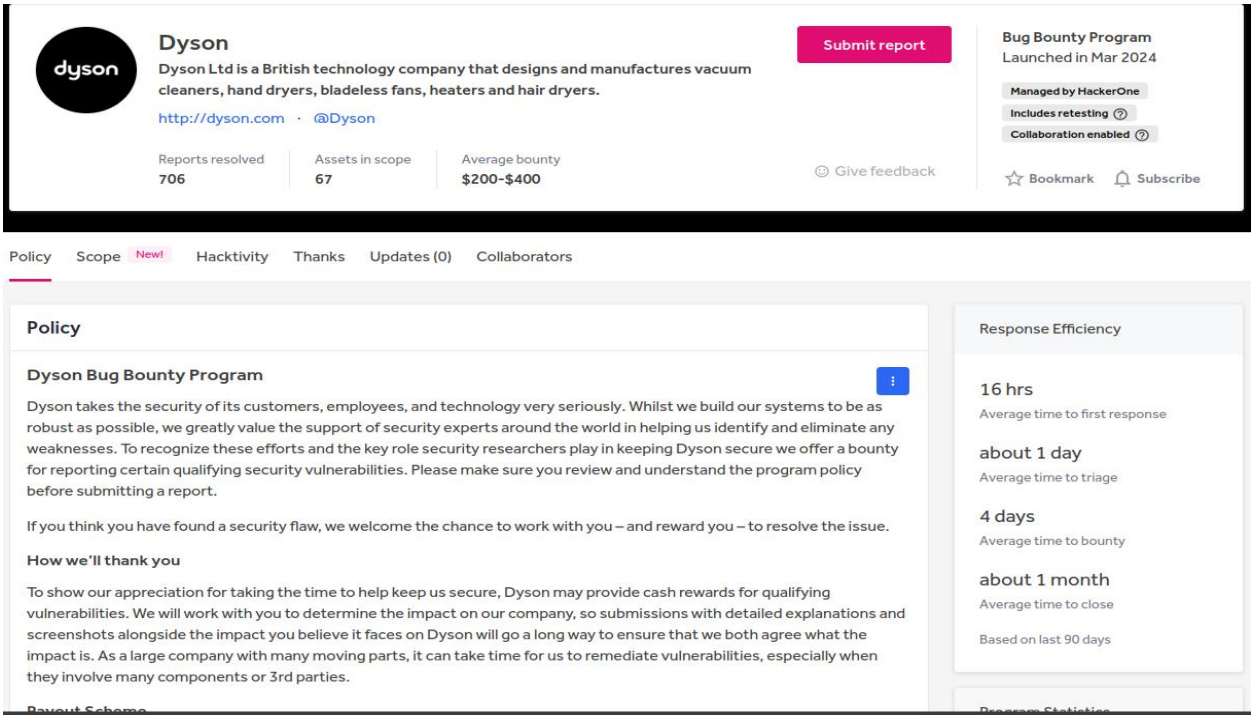
- Taking into account the application environment and business implications, these level concerns can be resolved.

6. Assignment scope

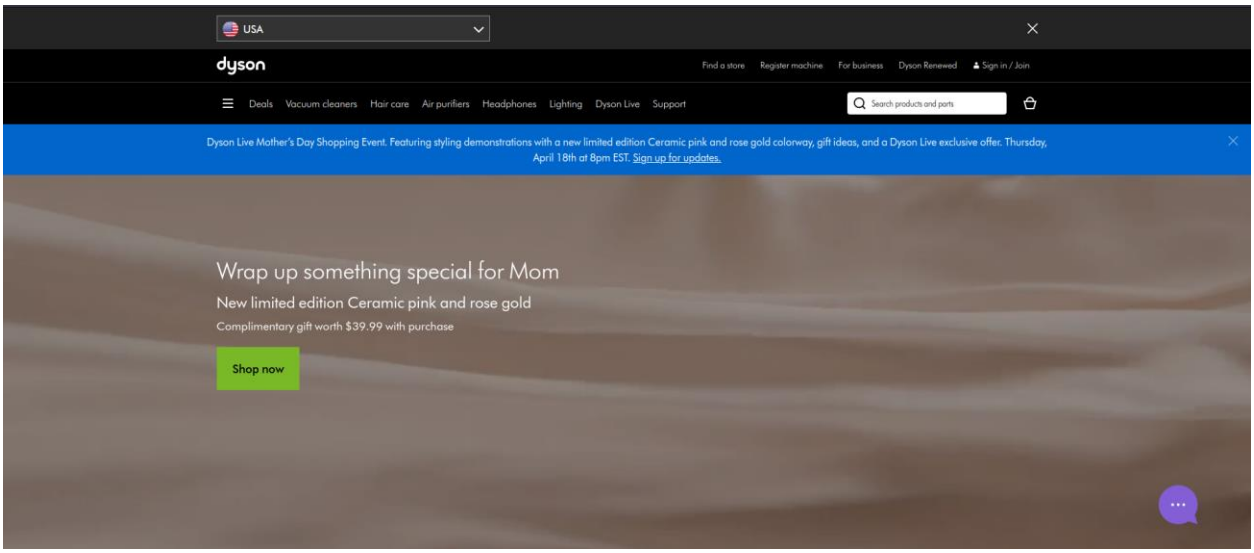
- Authentication
- Authorization
- Session Management
- Input Validation
- Encryption and cryptography
- Error Handling

Domain chooses to do the vulnerability scan http://dyson.com/

I have chosen this domain from hackerone website to see the policies, please visit, https://hackerone.com/dyson?type=team



7. Dyson



7.1. In scope domains

www.dyson.pt	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.no	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.fi.dyson.com	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.se	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.dk	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.nl	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.be	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.pt	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.no	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.de	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.ch	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.fr	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.ie	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.sa.dyson.com	Domain	In scope	Critical	Eligible	Jan 24, 2023
shop.dyson.ru	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.my	Domain	In scope	Critical	Eligible	Jan 24, 2023

www.dyson.fr	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.fi.dyson.com	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.co.th	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.it	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.de	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.cz	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.nl	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.co.uk	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.hu	Domain	In scope	Critical	Eligible	Jan 24, 2023
shop.dyson.co.za	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.at	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.com.ua	Domain	In scope	Critical	Eligible	Mar 12, 2024
www.dyson.ch	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.it	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.ie	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.es	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.com.tr	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.vn	Domain	In scope	Critical	Eligible	Jan 24, 2023
*.dyson.com	Other	In scope	Critical	Eligible	Aug 15, 2023
www.dyson.com.sg	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.co.uk	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.com	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.co.kr	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.be	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.co.il	Domain	In scope	Critical	Eligible	Jan 24, 2023
*.cp.dyson.com This namespace is used to publish API's relating to the registration and control of Dyson connected products.	Other	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.ae	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.co.nz	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dysoncanada.ca	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.com.ro	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.pl	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.in	Domain	In scope	Critical	Eligible	Jan 24, 2023

api.dysoncanada.ca	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.co.jp	Domain	In scope	Critical	Eligible	Jan 24, 2023
com.dyson.mobile.android (Dyson Link App - https://play.google.com/store/apps/details?id=com.dyson.mobile.android)	Android: Play Store	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.cn	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.com.mx	Domain	In scope	Critical	Eligible	Jan 24, 2023
api.dyson.com	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.dk	Domain	In scope	Critical	Eligible	Jan 24, 2023
New www.dyson.tw	Domain	In scope	Critical	Eligible	Updated Apr 10, 2024
api.dyson.es	Domain	In scope	Critical	Eligible	Jan 24, 2023
New shop.dyson.tw	Domain	In scope	Critical	Eligible	Updated Apr 10, 2024
api.dyson.at	Domain	In scope	Critical	Eligible	Jan 24, 2023
*.dyson.com	Wildcard	In scope	Critical	Eligible	Mar 7, 2024
www.dyson.com.au	Domain	In scope	Critical	Eligible	Jan 24, 2023
www.dyson.hk	Domain	In scope	Critical	Eligible	Jan 24, 2023

7.2. Out scope domains

mail.register-dyson.co.kr	Domain	Out of scope	None	Ineligible	Jan 24, 2023
test.oepay.dyson.cn	Domain	Out of scope	None	Ineligible	Jan 24, 2023
shop.dyson.co.kr	Domain	Out of scope	None	Ineligible	Jan 24, 2023
*central.dyson.com	Other	Out of scope	None	Ineligible	Jan 24, 2023
jamesdysonfoundation.*	Other	Out of scope	None	Ineligible	Jan 24, 2023
aio.shop.china-dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
q.dyson.cn	Domain	Out of scope	None	Ineligible	Jan 24, 2023
api.q.dyson.cn	Domain	Out of scope	None	Ineligible	Jan 24, 2023
fsc.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
auth.dysonrecall.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
centraltest.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
30secondbleeps.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
www.dyson.ovh	Domain	Out of scope	None	Ineligible	Jan 24, 2023
dysontherapie.fr	Domain	Out of scope	None	Ineligible	Jan 24, 2023
svn.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
sakti3.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023

svn.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
sakti3.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
on.dyson.co.uk	Domain	Out of scope	None	Ineligible	Jan 24, 2023
sm2.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
m.shop.dyson.cn	Domain	Out of scope	None	Ineligible	Jan 24, 2023
register-dyson.co.kr	Domain	Out of scope	None	Ineligible	Jan 24, 2023
jobs.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
reviews.dyson*	Other	Out of scope	None	Ineligible	Jan 24, 2023
sm3.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
view.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
central-test.dyson.com	Domain	Out of scope	None	Ineligible	Jan 24, 2023
community.dyson.com	Domain	Out of scope	None	Ineligible	Aug 15, 2023
careers.dyson.com	Domain	Out of scope	None	Ineligible	Feb 20, 2024
New *dyson-demo.com	Wildcard	Out of scope	None	Ineligible	Updated Apr 5, 2024

08. Bug Bounty Reports

Report 01

Target main Domain : http://dyson.com/

Information Gathering

Whois

In order to do a bug bounty first you must have the understanding about the web application that you choose. However all the above information is the information that the company provides us. But there are more to discover. So as the next step I decided to have a more deep look at this web application. For that I used "Whois" tool.

```
┌──(rasan㉿kali)-[~]
└─$ whois dyson.com
   Domain Name: DYSON.COM
   Registry Domain ID: 4785854_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2023-10-24T05:14:19Z
   Creation Date: 1997-10-29T05:00:00Z
   Registry Expiry Date: 2024-10-28T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: A1-82.AKAM.NET
   Name Server: A13-64.AKAM.NET
   Name Server: A2-65.AKAM.NET
   Name Server: A24-65.AKAM.NET
   Name Server: A4-67.AKAM.NET
   Name Server: A9-67.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-12T02:19:36Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
```

```
Domain Name: dyson.com
Registry Domain ID: 4785854_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-10-24T01:14:19Z
Creation Date: 1997-10-29T00:00:00Z
Registrar Registration Expiration Date: 2024-10-28T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Dyson Ltd
Registrant Street: Tetbury Hill
Registrant City: Wiltshire
Registrant State/Province:
Registrant Postal Code: SN16 0RP
Registrant Country: GB
Registrant Phone: +44.1666827200
Registrant Phone Ext:
Registrant Fax: +44.1666828040
Registrant Fax Ext:
Registrant Email: domainnames@dyson.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Dyson Ltd
Admin Street: Tetbury Hill
Admin City: Wiltshire
Admin State/Province:
Admin Postal Code: SN16 0RP
Admin Country: GB
Admin Phone: +44.1666827200
Admin Phone Ext:
Admin Fax: +44.1666828040
Admin Fax Ext:
Admin Email: domainnames@dyson.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Dyson Technology Limited
Tech Street: Tetbury Hill Malmesbury
Tech City: Wiltshire
Tech State/Province: ENG
Tech Postal Code: SN16 0RP
Tech Country: GB
```

```
Tech Postal Code: SN16 0RP
Tech Country: GB
Tech Phone: +44.1666827200
Tech Phone Ext:
Tech Fax: +44.1666828040
Tech Fax Ext:
Tech Email: domainnames@dyson.com
Name Server: a13-64.akam.net
Name Server: a2-65.akam.net
Name Server: a24-65.akam.net
Name Server: a9-67.akam.net
Name Server: a1-82.akam.net
Name Server: a4-67.akam.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-10-24T01:14:19Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC)  The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and Auction Monitoring, as well SSL Certificate Services
and DNS Hosting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or purposes of using the data in any manner that violates
these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. CSC
 does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: you agree that you may use this Data only for lawful purposes and that under no circumstances wil
l you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or facsimile; or (2) enable high
 volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS database in its sole discretion for any violations by you of th
ese terms of use. CSC reserves the right to modify these terms at any time.

Register your domain name at http://www.cscglobal.com
```

Then I used a tool to look at subdomains of Dyson.com. The tool I used is Sublist3r

Sublist3r

There are a few steps that can be followed to install sublist3r in Kali Linux.

- First download Sublist3r use this link https://github.com/aboul3la/Sublist3r.git and use the command in command prompt as
  $ git clone https://github.com/aboul3la/Sublist3r.git

- However, you need some requirements before installing sublist3r in your pc.

- As the first requirement python requirements such as requests, dnspython and argparse.

- So, to install python use the command given bellow.
  $ sudo pip install -r requirements.txt

```
┌──(rasan㉿kali)-[~/Desktop/Sublist3r]
└─$ sudo pip install -r requirements.txt
[sudo] password for rasan:
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.3.0)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.28.1)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package
rnings/venv
```

- Next install the requirement as follow

  - for install requests
  $ sudo apt-get install python-request

```
┌──(rasan㉿kali)-[~/Desktop/Sublist3r]
└─$ sudo apt-get install python-request
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
E: Unable to locate package python-request
```

- $ sudo pip install dnspython

```
┌──(rasan㉿kali)-[~/Desktop/Sublist3r]
└─$ sudo pip install dnspython
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (2.3.0)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting
rnings/venv
```

It had been already installed.

- $ sudo pip install argparse

```
┌──(rasan㉿kali)-[~/Desktop/Sublist3r]
└─$ sudo pip install argparse
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl.metadata (2.8 kB)
Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the syst
rnings/venv
```

- Now you can language Sublist3r using the bellow command.

$ python3 sublist3r.py -h

```
┌──(rasan㉿kali)-[~/Desktop/Sublist3r]
└─$ python3 sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python sublist3r.py -d google.com
```

- Now sublist3r is ready to use.
- To find the sub domains of the target domain use the bellow command. I am targeting "dyson.com".
  $ python3 sublist3r.py -d dyson.com

```
┌──(rasan㉿kali)-[~/Desktop/Sublist3r]
└─$ python3 sublist3r.py -d dyson.com

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for dyson.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 642
www.dyson.com
AWCONTENT-APAC.dyson.com
AWCONTENT-EMEA.dyson.com
AWSEG-APAC.dyson.com
AWSEG-AU.dyson.com
AWSEG-EMEA.dyson.com
AWTUNNEL-APAC.dyson.com
AWTUNNEL-EMEA.dyson.com
Jobs.dyson.com
Loadtest.dyson.com
Lyncdiscover.dyson.com
Lyncdiscoverinternal.dyson.com
Lyncweb.dyson.com
Media.dyson.com
Oneview.dyson.com
Qtest.dyson.com
Webconf.dyson.com
Webmail-JP.dyson.com
```

```
Webconf.dyson.com
Webmail-JP.dyson.com
Webmail-SG.dyson.com
Webmail-US.dyson.com
aadsldaps.dyson.com
access-jp.dyson.com
access-my.dyson.com
access-one.dyson.com
access-one-project.dyson.com
access-sg.dyson.com
access-uk.dyson.com
access-uk-genius.dyson.com
access-uk-group.dyson.com
access-uk-local.dyson.com
access-uk-mdm.dyson.com
access-uk-mdmdev.dyson.com
access-uk-me.dyson.com
access-uk-motor.dyson.com
access-uk-project.dyson.com
access-uk-search.dyson.com
access-us.dyson.com
adminqaservice.dyson.com
adminservice.dyson.com
akamai.dyson.com
origin.akamai.dyson.com
api.dyson.com
api-alexa-login.dyson.com
api-machine.dyson.com
www.ar.dyson.com
auth.dyson.com
autodiscover.dyson.com
av.dyson.com
av-sg.dyson.com
avau.dyson.com
avsg.dyson.com
avuk.dyson.com
avus.dyson.com
avus2.dyson.com
b2bapp.dyson.com
authoring.b2bapp.dyson.com
beta.dyson.com
betatrial.dyson.com
build.dyson.com
business.dyson.com
```

```
www.careers.dyson.com
censhare.dyson.com
www.censhare.dyson.com
central.dyson.com
www.central.dyson.com
centraltest.dyson.com
www.centraltest.dyson.com
cheetah-au.dyson.com
cheetah-cn.dyson.com
cheetah-jp.dyson.com
cheetah-sg.dyson.com
cheetah-uk.dyson.com
cheetah-us.dyson.com
cmcontroltower.dyson.com
communit.dyson.com
www.communit.dyson.com
community.dyson.com
www.community.dyson.com
commvault-test.dyson.com
gwr.perf.connected.dyson.com
gwr.ppe.connected.dyson.com
gwr.prd.connected.dyson.com
gwr.si.connected.dyson.com
gwr.stg.connected.dyson.com
gwr.uat.connected.dyson.com
connectedgwr.dyson.com
content.dyson.com
contentfi.dyson.com
cost-calculator.dyson.com
cp.dyson.com
api.cp.dyson.com
appapi.cp.dyson.com
appapigw.cp.dyson.com
auth.cp.dyson.com
dsr.c3.cp.dyson.com
launcher.c3.cp.dyson.com
ota.c3.cp.dyson.com
servicetool.c3.cp.dyson.com
srg.c3.cp.dyson.com
cfappapi.cp.dyson.com
cfmachinegw.cp.dyson.com
cfqr.cp.dyson.com
console.cp.dyson.com
gwr.cp.dyson.com
```

```
lec-mcs.cpci.dyson.com
partnerapi.cpci.dyson.com
qr.cpci.dyson.com
statuspage.cpci.dyson.com
api.cpcommon-dev.dyson.com
appapi.cpcommon-dev.dyson.com
console.cpcommon-dev.dyson.com
partnerapi.cpcommon-dev.dyson.com
qr.cpcommon-dev.dyson.com
gwr.cpdev.dyson.com
api.cpdev000.dyson.com
appapi.cpdev000.dyson.com
appapigw.cpdev000.dyson.com
appbroker1.cpdev000.dyson.com
auth.cpdev000.dyson.com
cfqr.cpdev000.dyson.com
console.cpdev000.dyson.com
gwr.cpdev000.dyson.com
partnerapi.cpdev000.dyson.com
qr.cpdev000.dyson.com
statuspage.cpdev000.dyson.com
cpdev001.dyson.com
api.cpdev001.dyson.com
appapi.cpdev001.dyson.com
appapigw.cpdev001.dyson.com
auth.cpdev001.dyson.com
cfqr.cpdev001.dyson.com
console.cpdev001.dyson.com
gwr.cpdev001.dyson.com
idpm.cpdev001.dyson.com
partnerapi.cpdev001.dyson.com
qr.cpdev001.dyson.com
cpdev002.dyson.com
agappapi.cpdev002.dyson.com
agcfappapi.cpdev002.dyson.com
albgwapi.cpdev002.dyson.com
api.cpdev002.dyson.com
apiru.cpdev002.dyson.com
appapi.cpdev002.dyson.com
appapi2.cpdev002.dyson.com
appapi3.cpdev002.dyson.com
appapigw.cpdev002.dyson.com
appgateway.cpdev002.dyson.com
auth.cpdev002.dyson.com
```

```
backendapi.cpdev002.dyson.com
cfalbgwapi.cpdev002.dyson.com
cfappapi.cpdev002.dyson.com
cfappapigw.cpdev002.dyson.com
cfbroker1.cpdev002.dyson.com
cfmachinegw.cpdev002.dyson.com
dyson.comappapi.cpdev002.dyson.com
console.cpdev002.dyson.com
cr-app-api.cpdev002.dyson.com
dc-api.cpdev002.dyson.com
dcappapi.cpdev002.dyson.com
dccfappapi.cpdev002.dyson.com
gateway.cpdev002.dyson.com
gwappapi.cpdev002.dyson.com
gwcfappapi.cpdev002.dyson.com
gwr.cpdev002.dyson.com
machineapi.cpdev002.dyson.com
notappapi.cpdev002.dyson.com
partnerapi.cpdev002.dyson.com
qr.cpdev002.dyson.com
scheduleapi.cpdev002.dyson.com
statuspage.cpdev002.dyson.com
testappapi.cpdev002.dyson.com
userapi.cpdev002.dyson.com
cpdev003.dyson.com
api.cpdev003.dyson.com
appapi.cpdev003.dyson.com
appapigw.cpdev003.dyson.com
auth.cpdev003.dyson.com
dsr.c3.cpdev003.dyson.com
launcher.c3.cpdev003.dyson.com
provisioningstatus.c3.cpdev003.dyson.com
console.cpdev003.dyson.com
gwr.cpdev003.dyson.com
gwr-test.cpdev003.dyson.com
interapi.cpdev003.dyson.com
lec-mcs.cpdev003.dyson.com
partnerapi.cpdev003.dyson.com
qr.cpdev003.dyson.com
cpdev004.dyson.com
apple.adminapp.cpdev004.dyson.com
apple1.adminapp.cpdev004.dyson.com
launcher.adminapp.cpdev004.dyson.com
launchers.adminapp.cpdev004.dyson.com
```

```
productcare.adminapp.cpdev004.dyson.com
amfr.cpdev004.dyson.com
api.cpdev004.dyson.com
appapi.cpdev004.dyson.com
appapigw.cpdev004.dyson.com
auth.c3.cpdev004.dyson.com
launcher.c3.cpdev004.dyson.com
launchers.c3.cpdev004.dyson.com
mds.c3.cpdev004.dyson.com
midastool.c3.cpdev004.dyson.com
ota.c3.cpdev004.dyson.com
servicetool.c3.cpdev004.dyson.com
stl571.c3.cpdev004.dyson.com
test.c3.cpdev004.dyson.com
test1.c3.cpdev004.dyson.com
console.cpdev004.dyson.com
gwr.cpdev004.dyson.com
idpm.cpdev004.dyson.com
interapi.cpdev004.dyson.com
partnerapi.cpdev004.dyson.com
qr.cpdev004.dyson.com
sp.cpdev004.dyson.com
statuspage.cpdev004.dyson.com
test.cpdev004.dyson.com
acm.test.cpdev004.dyson.com
api.cpeqdev.dyson.com
appapi.cpeqdev.dyson.com
appapigw.cpeqdev.dyson.com
console.cpeqdev.dyson.com
eq-kf-cognito.cpeqdev.dyson.com
kf.cpeqdev.dyson.com
auth.kf.cpeqdev.dyson.com
kubeflow.cpeqdev.dyson.com
auth.kubeflow.cpeqdev.dyson.com
partnerapi.cpeqdev.dyson.com
qr.cpeqdev.dyson.com
testkf.cpeqdev.dyson.com
api.cpimgclass-dev.dyson.com
appapi.cpimgclass-dev.dyson.com
partnerapi.cpimgclass-dev.dyson.com
api.cpimgclass-prd.dyson.com
appapi.cpimgclass-prd.dyson.com
partnerapi.cpimgclass-prd.dyson.com
agappapi.cplt.dyson.com
```

```
api.cpppe.dyson.com
appapi.cpppe.dyson.com
appapigw.cpppe.dyson.com
auth.cpppe.dyson.com
dsr.c3.cpppe.dyson.com
launcher.c3.cpppe.dyson.com
ota.c3.cpppe.dyson.com
servicetool.c3.cpppe.dyson.com
srg.c3.cpppe.dyson.com
cfappapi.cpppe.dyson.com
cfmachinegw.cpppe.dyson.com
cfqr.cpppe.dyson.com
console.cpppe.dyson.com
gwr.cpppe.dyson.com
interapi.cpppe.dyson.com
lec-mcs.cpppe.dyson.com
partnerapi.cpppe.dyson.com
qr.cpppe.dyson.com
statuspage.cpppe.dyson.com
gwr.cpqa.dyson.com
partnerapi.cpqa.dyson.com
cpsi.dyson.com
agappapi.cpsi.dyson.com
agcfappapi.cpsi.dyson.com
amok.cpsi.dyson.com
api.cpsi.dyson.com
appapi.cpsi.dyson.com
appapigw.cpsi.dyson.com
auth.cpsi.dyson.com
dsr.c3.cpsi.dyson.com
launcher.c3.cpsi.dyson.com
ota.c3.cpsi.dyson.com
servicetool.c3.cpsi.dyson.com
srg.c3.cpsi.dyson.com
cfappapi.cpsi.dyson.com
cfmachinegw.cpsi.dyson.com
cfqr.cpsi.dyson.com
console.cpsi.dyson.com
gwr.cpsi.dyson.com
interapi.cpsi.dyson.com
lec-mcs.cpsi.dyson.com
n276-eb1-trial.cpsi.dyson.com
partnerapi.cpsi.dyson.com
qr.cpsi.dyson.com
```

```
dev-splunk-heavy-forwarder-hec-external.cptools.dyson.com
jenkins.cptools.dyson.com
jenkins-ecs.cptools.dyson.com
prod-splunk-heavy-forwarder-hec-external.cptools.dyson.com
artifactory.cptoolsdev.dyson.com
artifactory-temp.cptoolsdev.dyson.com
artifactory-test.cptoolsdev.dyson.com
dev-splunk-heavy-forwarder-hec-external.cptoolsdev.dyson.com
jenkins.cptoolsdev.dyson.com
jenkins-ecs.cptoolsdev.dyson.com
prod-splunk-heavy-forwarder-hec-external.cptoolsdev.dyson.com
gwr.cptrials.dyson.com
agappapi.cpuat.dyson.com
agcfappapi.cpuat.dyson.com
appapi.cpuat.dyson.com
cfappapi.cpuat.dyson.com
gwr.cpuat.dyson.com
partnerapi.cpuat.dyson.com
daybook.dyson.com
demo3D.dyson.com
www.demo3D.dyson.com
desktop.dyson.com
desktop-my.dyson.com
desktop-sea.dyson.com
deu-lt02.dyson.com
devices.dyson.com
dhs.dyson.com
www.dhs.dyson.com
dialin.dyson.com
dialinsg.dyson.com
dialinuk.dyson.com
mail01.digital.dyson.com
mail02.digital.dyson.com
digitalsupport.dyson.com
vertex.dldev.dyson.com
oeam.dlsit.dyson.com
resolve.dlsit.dyson.com
resolve-api.dlsit.dyson.com
docminder.dyson.com
www.docminder.dyson.com
www.dpsc.dyson.com
dre.dyson.com
api.dre.dyson.com
drtvlive.dyson.com
```

```
api.dre.dyson.com
drtvlive.dyson.com
dysoncmg.dyson.com
click.e.dyson.com
cloud.e.dyson.com
image.e.dyson.com
view.e.dyson.com
elearning.dyson.com
www.elearning.dyson.com
engage.dyson.com
engageapi.dyson.com
engageimportapi.dyson.com
engagetrain.dyson.com
engagetrainapi.dyson.com
engagetrainimportapi.dyson.com
epm.dyson.com
epm-test.dyson.com
staging.admin.uu.eu.dyson.com
staging.uu.eu.dyson.com
extend.dyson.com
feedback.dyson.com
www.fi.dyson.com
api.fi.dyson.com
beta.fi.dyson.com
shop.fi.dyson.com
www.shop.fi.dyson.com
forbusiness-preferences.dyson.com
www.forbusiness-preferences.dyson.com
gbr-lt02.dyson.com
genius.dyson.com
genius-sg.dyson.com
genius-test.dyson.com
genius-us.dyson.com
content.global.dyson.com
www.gr.dyson.com
group.dyson.com
group-test.dyson.com
gtm.dyson.com
hnsc-us.dyson.com
id.dyson.com
api.id.dyson.com
identity-hub.dyson.com
idp.dyson.com
idp-debug.dyson.com
```

```
idp-home.dyson.com
idp-test.dyson.com
idp-test-help.dyson.com
imap.dyson.com
irc-portal.dyson.com
ircpp.dyson.com
www.isseymiyake.dyson.com
jamf.dyson.com
jobs.dyson.com
www.jobs.dyson.com
jpn-lt02.dyson.com
kr.dyson.com
www.kr.dyson.com
registration.kr.dyson.com
shop.kr.dyson.com
admin.shop.kr.dyson.com
staging.admin.shop.kr.dyson.com
staging2.admin.shop.kr.dyson.com
staging.shop.kr.dyson.com
staging2.shop.kr.dyson.com
support.kr.dyson.com
www.krefel.dyson.com
www.kz.dyson.com
landscape.dyson.com
www.lb.dyson.com
learning.dyson.com
legacy.dyson.com
linkapp-api.dyson.com
linkserver-api.dyson.com
loadtest.dyson.com
local.dyson.com
local-sg.dyson.com
local-test.dyson.com
local-us.dyson.com
lync.dyson.com
lync-sg.dyson.com
www.lync-sg.dyson.com
lyncdiscover.dyson.com
lyncdiscoverinternal.dyson.com
lyncweb.dyson.com
lyncweb-my.dyson.com
lyncweb-sg.dyson.com
lyncweb-us.dyson.com
jenkins.magento.dyson.com
```

```
me-sg.dyson.com
me-test.dyson.com
me-us.dyson.com
media.dyson.com
meet.dyson.com
meet-sg.dyson.com
meetsg.dyson.com
meetuk.dyson.com
mobile-admin.dyson.com
motor.dyson.com
motor-sg.dyson.com
motor-test.dyson.com
motor-us.dyson.com
officewa-au.dyson.com
officewa-sg.dyson.com
officewa-uk.dyson.com
officewa-uk-test.dyson.com
officewa-us.dyson.com
oldmedia.dyson.com
oneview.dyson.com
pi-pro.dyson.com
ae.preprod.dyson.com
au.preprod.dyson.com
cz.preprod.dyson.com
dysonsandbox.preprod.dyson.com
hk.preprod.dyson.com
hk2.preprod.dyson.com
hu.preprod.dyson.com
il.preprod.dyson.com
in.preprod.dyson.com
kr.preprod.dyson.com
leapcms.preprod.dyson.com
lmdyson.preprod.dyson.com
mx.preprod.dyson.com
mx2.preprod.dyson.com
my.preprod.dyson.com
nz.preprod.dyson.com
pl.preprod.dyson.com
ro.preprod.dyson.com
sa.preprod.dyson.com
sg.preprod.dyson.com
sg2.preprod.dyson.com
th.preprod.dyson.com
tr.preprod.dyson.com
```

```
th.preprod.dyson.com
tr.preprod.dyson.com
tr2.preprod.dyson.com
vn.preprod.dyson.com
za.preprod.dyson.com
www.press.dyson.com
privacy.dyson.com
project.dyson.com
project-sg.dyson.com
project-test.dyson.com
project-us.dyson.com
qastubs.dyson.com
qtest.dyson.com
qtest-staging.dyson.com
queue.dyson.com
registration.dyson.com
api.registration.dyson.com
gwr.registration.dyson.com
remote-rvd.dyson.com
remote-vdi.dyson.com
reviews.dyson.com
rspro.dyson.com
www.rspro.dyson.com
rsqas.dyson.com
www.rsqas.dyson.com
s2pc.dyson.com
s4herpcs01c.dyson.com
www.s4herpcs01c.dyson.com
s4hq44app01v.dyson.com
www.s4hq44app01v.dyson.com
sa.dyson.com
www.sa.dyson.com
admin.sa.dyson.com
staging.admin.sa.dyson.com
forbusiness.sa.dyson.com
staging.sa.dyson.com
support.sa.dyson.com
saa.dyson.com
safetyreporting.dyson.com
www.safetyreporting.dyson.com
api.safetyreporting.dyson.com
www.api.safetyreporting.dyson.com
development.api.safetyreporting.dyson.com
www.development.api.safetyreporting.dyson.com
```

```
staging.safetyreporting.dyson.com
www.staging.safetyreporting.dyson.com
www.sales.dyson.com
wildcard.san.dyson.com
scc.dyson.com
sccscnapp01v.dyson.com
www.sccscnapp01v.dyson.com
sccscpapp01v.dyson.com
www.sccscpapp01v.dyson.com
sea.dyson.com
search.dyson.com
search-us.dyson.com
selfresolve.dyson.com
selfresolve-UAT.dyson.com
service.dyson.com
sfbsg.dyson.com
sip.dyson.com
www.sip.dyson.com
sipau.dyson.com
sipsg.dyson.com
sipuk.dyson.com
sipus.dyson.com
sipus2.dyson.com
skypewebau.dyson.com
skypewebmy.dyson.com
skypewebsg.dyson.com
skypewebuk.dyson.com
skypewebus.dyson.com
skypewebus2.dyson.com
snow-gateway.dyson.com
www.snow-gateway.dyson.com
social-test.dyson.com
staging-demo3D.dyson.com
www.staging-demo3D.dyson.com
tableau.dyson.com
tableauchina.dyson.com
tableaudev.dyson.com
tableauqas.dyson.com
tandcs.dyson.com
teamcenter.dyson.com
teamcenterMY.dyson.com
teamcenterSG.dyson.com
teamcenterUK.dyson.com
teamcenterUK-DEV.dyson.com
```

```
www.snow-gateway.dyson.com
social-test.dyson.com
staging-demo3D.dyson.com
www.staging-demo3D.dyson.com
tableau.dyson.com
tableauchina.dyson.com
tableaudev.dyson.com
tableauqas.dyson.com
tandcs.dyson.com
teamcenter.dyson.com
teamcenterMY.dyson.com
teamcenterSG.dyson.com
teamcenterUK.dyson.com
teamcenterUK-DEV.dyson.com
telescope.dyson.com
www.telescope.dyson.com
test.dyson.com
tracking.dyson.com
retail.trainingacademy.dyson.com
uk-mal-ise-adm.dyson.com
www.uk-mal-ise-adm.dyson.com
uk-mal-ise-adm-01.dyson.com
upgrade.dyson.com
webconf.dyson.com
webconf-sg.dyson.com
webconfau.dyson.com
webconfsg.dyson.com
webconfuk.dyson.com
webconfus.dyson.com
webconfus2.dyson.com
webmail.dyson.com
www.webmail.dyson.com
webmail-au.dyson.com
webmail-jp.dyson.com
webmail-my.dyson.com
webmail-sg.dyson.com
webmail-us.dyson.com
webmaildr.dyson.com
webmailtest.dyson.com
xyz.dyson.com
www.getdyson.com
```

Recon -ng Tool

Recon-ng is versatile and powerful reconnaissance tool used by penetration testers, security analysts and researchers to gather valuable information about targets and assess their security posture. However, it's important to use Recon-ng responsibly and within legal boundaries respecting the privacy and security of targeted system and individuals.

Installation

GitHub link - https://github.com/lanmaster53/recon-ng

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ git clone https://github.com/lanmaster53/recon-ng
Cloning into 'recon-ng'...
remote: Enumerating objects: 9522, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 9522 (delta 3), reused 14 (delta 3), pack-reused 9503
Receiving objects: 100% (9522/9522), 3.06 MiB | 1.68 MiB/s, done.
Resolving deltas: 100% (4958/4958), done.
```

Then open the recon-ng directory and install it using following command

$ pip install -r REQUIREMENTS

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ cd recon-ng

┌──(rasan㉿kali)-[~/Desktop/recon-ng]
└─$ ls
docker-compose.yml  LICENSE    recon      recon-ng   REQUIREMENTS
Dockerfile          README.md  recon-cli  recon-web  VERSION

┌──(rasan㉿kali)-[~/Desktop/recon-ng]
└─$ pip install -r REQUIREMENTS
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 2))
(6.0)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 3
)) (2.3.0)
Requirement already satisfied: lxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 4)) (4
.9.2)
Requirement already satisfied: mechanize in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 5
)) (0.4.8)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 6)
) (2.28.1)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 8)) (
2.2.2)
Requirement already satisfied: flask-restful in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (li
ne 9)) (0.3.9)
Requirement already satisfied: flasgger in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 10
)) (0.9.5)
Requirement already satisfied: dicttoxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 1
1)) (1.7.15)
Requirement already satisfied: XlsxWriter in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line
12)) (3.0.2)
Requirement already satisfied: unicodecsv in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line
13)) (0.14.1)
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.
13.0)
```

Proof of concept

To run recon-ng type following command and press enter

```
┌──(rasan㉿kali)-[~/Desktop/recon-ng]
└─$ recon-ng
[*] Version check disabled.

   _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/          _/      _/    _/_/_/
  _/    _/  _/        _/        _/      _/  _/_/    _/          _/_/    _/  _/
 _/_/_/    _/_/_/    _/        _/      _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
_/    _/  _/        _/        _/      _/  _/    _/_/          _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/          _/      _/    _/_/_/


                                   ^
                                  / \\ ^
    Sponsored by ...            ^  /\/  \\v  \/\
                               / \\/ // \\\\\ \\ \/\
                              // // BLACK HILLS V \\
                             www.blackhillsinfosec.com

                 ___  ___  ___  ___ ____ _ ___  ___ ___
                |___] |__/ |___| |     |  | |__  |__ |
                |    |  \_ |   | |___  |  |  ___| |___ |___
                             www.practisec.com

                       [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] >
```

In here no any modules installed therefore we want to install the modules using marketplace keyword.

```
[*] No modules enabled/installed.

[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
[*] Module installed: recon/contacts-credentials/hibp_breach
[*] Module installed: recon/contacts-credentials/hibp_paste
[*] Module installed: recon/contacts-domains/migrate_contacts
[*] Module installed: recon/contacts-profiles/fullcontact
[*] Module installed: recon/credentials-credentials/adobe
[*] Module installed: recon/credentials-credentials/bozocrack
[*] Module installed: recon/credentials-credentials/hashes_org
[*] Module installed: recon/domains-companies/censys_companies
[*] Module installed: recon/domains-companies/pen
[*] Module installed: recon/domains-companies/whoxy_whois
[*] Module installed: recon/domains-contacts/hunter_io
[*] Module installed: recon/domains-contacts/metacrawler
[*] Module installed: recon/domains-contacts/pen
[*] Module installed: recon/domains-contacts/pgp_search
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/wikileaker
[*] Module installed: recon/domains-credentials/pwnedlist/account_cred
[*] Module installed: recon/domains-credentials/pwnedlist/api_usage
[*] Module installed: recon/domains-credentials/pwnedlist/domain_creds
```

```
[*] Module installed: recon/domains-credentials/pwnedlist/domain_ispwned
[*] Module installed: recon/domains-credentials/pwnedlist/leak_lookup
[*] Module installed: recon/domains-credentials/pwnedlist/leaks_dump
[*] Module installed: recon/domains-domains/brute_suffix
[*] Module installed: recon/domains-hosts/binaryedge
[*] Module installed: recon/domains-hosts/bing_domain_api
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/brute_hosts
[*] Module installed: recon/domains-hosts/builtwith
[*] Module installed: recon/domains-hosts/censys_domain
[*] Module installed: recon/domains-hosts/certificate_transparency
[*] Module installed: recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/mx_spf_ip
[*] Module installed: recon/domains-hosts/netcraft
[*] Module installed: recon/domains-hosts/shodan_hostname
[*] Module installed: recon/domains-hosts/spyse_subdomains
[*] Module installed: recon/domains-hosts/ssl_san
[*] Module installed: recon/domains-hosts/threatcrowd
[*] Module installed: recon/domains-hosts/threatminer
[*] Module installed: recon/domains-vulnerabilities/ghdb
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Module installed: recon/hosts-domains/migrate_hosts
[*] Module installed: recon/hosts-hosts/bing_ip
[*] Module installed: recon/hosts-hosts/censys_hostname
[*] Module installed: recon/hosts-hosts/censys_ip
[*] Module installed: recon/hosts-hosts/censys_query
[*] Module installed: recon/hosts-hosts/ipinfodb
[*] Module installed: recon/hosts-hosts/ipstack
[*] Module installed: recon/hosts-hosts/resolve
[*] Module installed: recon/hosts-hosts/reverse_resolve
[*] Module installed: recon/hosts-hosts/ssltools
[*] Module installed: recon/hosts-hosts/virustotal
[*] Module installed: recon/hosts-locations/migrate_hosts
[*] Module installed: recon/hosts-ports/binaryedge
[*] Module installed: recon/hosts-ports/shodan_ip
[*] Module installed: recon/locations-locations/geocode
[*] Module installed: recon/locations-locations/reverse_geocode
[*] Module installed: recon/locations-pushpins/flickr
[*] Module installed: recon/locations-pushpins/shodan
[*] Module installed: recon/locations-pushpins/twitter
[*] Module installed: recon/locations-pushpins/youtube
[*] Module installed: recon/netblocks-companies/censys_netblock_company
[*] Module installed: recon/netblocks-companies/whois_orgs
[*] Module installed: recon/netblocks-hosts/censys_netblock
```

```
[*] Module installed: recon/locations-locations/reverse_geocode
[*] Module installed: recon/locations-pushpins/flickr
[*] Module installed: recon/locations-pushpins/shodan
[*] Module installed: recon/locations-pushpins/twitter
[*] Module installed: recon/locations-pushpins/youtube
[*] Module installed: recon/netblocks-companies/censys_netblock_company
[*] Module installed: recon/netblocks-companies/whois_orgs
[*] Module installed: recon/netblocks-hosts/censys_netblock
[*] Module installed: recon/netblocks-hosts/reverse_resolve
[*] Module installed: recon/netblocks-hosts/shodan_net
[*] Module installed: recon/netblocks-hosts/virustotal
[*] Module installed: recon/netblocks-ports/census_2012
[*] Module installed: recon/netblocks-ports/censysio
[*] Module installed: recon/ports-hosts/migrate_ports
[*] Module installed: recon/ports-hosts/ssl_scan
[*] Module installed: recon/profiles-contacts/bing_linkedin_contacts
[*] Module installed: recon/profiles-contacts/dev_diver
[*] Module installed: recon/profiles-contacts/github_users
[*] Module installed: recon/profiles-profiles/namechk
[*] Module installed: recon/profiles-profiles/profiler
[*] Module installed: recon/profiles-profiles/twitter_mentioned
[*] Module installed: recon/profiles-profiles/twitter_mentions
[*] Module installed: recon/profiles-repositories/github_repos
[*] Module installed: recon/repositories-profiles/github_commits
[*] Module installed: recon/repositories-vulnerabilities/gists_search
[*] Module installed: recon/repositories-vulnerabilities/github_dorks
[*] Module installed: reporting/csv
[*] Module installed: reporting/html
[*] Module installed: reporting/json
[*] Module installed: reporting/list
[*] Module installed: reporting/proxifier
[*] Module installed: reporting/pushpin
[*] Module installed: reporting/xlsx
[*] Module installed: reporting/xml
[*] Reloading modules ...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[!] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
```

Then we try to check subdomain in Brute force.

```
[recon-ng][default] > module search brute
[!] Invalid command: module search brute.
[recon-ng][default] > modules search brute
[*] Searching installed modules for 'brute'...

  Exploitation
  ------------

    exploitation/injection/xpath_bruter

  Recon
  -----

    recon/domains-domains/brute_suffix
    recon/domains-hosts/brute_hosts

[recon-ng][default] > workspaces create test
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[!] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_api' key not set. ipstack module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_ip module will likely fail at runtime. See 'keys add'.
[!] 'ipinfodb_api' key not set. ipinfodb module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/hosts-hosts/censys_hostname' disabled. Dependency required: 'me 'CensysIPv4' from 'cen
sys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] Module 'recon/hosts-hosts/censys_ip' disabled. Dependency required: 'me 'CensysIPv4' from 'censys.se
arch' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] Module 'recon/hosts-hosts/censys_query' disabled. Dependency required: 'me 'CensysIPv4' from 'censys
.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'spyse_api' key not set. spyse_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-hosts/censys_domain' disabled. Dependency required: 'me 'CensysIPv4' from 'cen
sys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
```

```
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[recon-ng][test] > modules load recon/domains-hosts/brute_hosts
[recon-ng][test][brute_hosts] > options
Manages the current context options

Usage: options <list|set|unset> [ ... ]

[recon-ng][test][brute_hosts] > options list

  Name      Current Value                          Required  Description
  ---------- -------------                          --------  -----------
  SOURCE    default                                yes       source of input (see 'info' for details)
  WORDLIST  /home/rasan/.recon-ng/data/hostnames.txt  yes       path to hostname wordlist

[recon-ng][test][brute_hosts] > options set SOURCE dyson.com
SOURCE => dyson.com
[recon-ng][test][brute_hosts] > run

--------
DYSON.COM
--------
[*] Wildcard DNS entry found for 'dyson.com' at '52.59.125.242'.
[*] 0.dyson.com => Response matches the wildcard.
[*] 03.dyson.com => (A) 52.59.122.122
[*] 01.dyson.com => Response matches the wildcard.
[*] 11.dyson.com => (A) 52.59.122.122
[*] 10.dyson.com => Response matches the wildcard.
[*] 02.dyson.com => Response matches the wildcard.
[*] 13.dyson.com => Response matches the wildcard.
[*] Country: None
[*] 14.dyson.com => Response matches the wildcard.
[*] Host: 11.dyson.com
[*] Ip_Address: 52.59.122.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] 11.dyson.com => (A) 52.59.125.242
[*] Country: None
[*] Host: 11.dyson.com
[*] Ip_Address: 52.59.125.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Country: None
[*] Host: 03.dyson.com
[*] Ip_Address: 52.59.122.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] 03.dyson.com => (A) 52.59.125.242
[*] Country: None
[*] Host: 03.dyson.com
[*] Ip_Address: 52.59.125.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] 15.dyson.com => (A) 52.59.122.122
[*] Country: None
[*] Host: 15.dyson.com
[*] Ip_Address: 52.59.122.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] 15.dyson.com => (A) 52.59.125.242
[*] Country: None
[*] Host: 15.dyson.com
[*] Ip_Address: 52.59.125.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] 16.dyson.com => Response matches the wildcard.
[*] 17.dyson.com => (A) 52.59.122.122
[*] Country: None
[*] Host: 17.dyson.com
[*] Ip_Address: 52.59.122.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] 17.dyson.com => (A) 52.59.125.242
```

```
[*] ----------
[*] ws.dyson.com => (A) 52.59.122.122
[*] Country: None
[*] Host: ws.dyson.com
[*] Ip_Address: 52.59.122.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] ws.dyson.com => (A) 52.59.125.242
[*] Country: None
[*] Host: ws.dyson.com
[*] Ip_Address: 52.59.125.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] zw.dyson.com => (A) 52.59.122.122
[*] Country: None
[*] Host: zw.dyson.com
[*] Ip_Address: 52.59.122.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] zw.dyson.com => (A) 52.59.125.242
[*] Country: None
[*] Host: zw.dyson.com
[*] Ip_Address: 52.59.125.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------

-------
SUMMARY
-------
[*] 1967 total (1949 new) hosts found.
[recon-ng][test][brute_hosts] > show hosts

  +----------------------------------------------------------------------+
```

```
[*] 1967 total (1949 new) hosts found.
[recon-ng][test][brute_hosts] > show hosts

  +-----------------------------------------------------------------------------------------------------------------------------------------+
-----------------------------------------+
  | rowid |                host                |     ip_address     | region | country | latitude | longitud
e | notes |     module    |
  +-----------------------------------------------------------------------------------------------------------------------------------------+
-----------------------------------------+
  | 1     | 11.dyson.com                       | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 2     | 11.dyson.com                       | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 3     | 03.dyson.com                       | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 4     | 03.dyson.com                       | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 5     | 15.dyson.com                       | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 6     | 15.dyson.com                       | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 7     | 17.dyson.com                       | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 8     | 17.dyson.com                       | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 9     | 19.dyson.com                       | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 10    | 2.dyson.com                        | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 11    | 2.dyson.com                        | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 12    | 19.dyson.com                       | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 13    | 3.dyson.com                        | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 14    | 3.dyson.com                        | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 15    | 3com.dyson.com                     | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 16    | 3com.dyson.com                     | 52.59.125.242      |        |         |          |
  |       | brute_hosts |
  | 17    | 5.dyson.com                        | 52.59.122.122      |        |         |          |
  |       | brute_hosts |
  | 18    | 5.dyson.com                        | 52.59.125.242      |        |         |          |
```

```
| 978  | master.dyson.com              | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 979  | max.dyson.com                 | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 980  | max.dyson.com                 | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 981  | md.dyson.com                  | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 982  | md.dyson.com                  | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 983  | me.dyson.com                  | 62.189.28.143  |  |  |  |
|      | brute_hosts |
| 984  | members.dyson.com             | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 985  | members.dyson.com             | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 986  | mercury.dyson.com             | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 987  | mercury.dyson.com             | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 988  | merlin.dyson.com              | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 989  | merlin.dyson.com              | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 990  | www2.dyson.com.edgekey.net    |  |  |  |  |
|      | brute_hosts |
| 991  | media.dyson.com               |  |  |  |  |
|      | brute_hosts |
| 992  | media.dyson.com               | 23.223.45.195  |  |  |  |
|      | brute_hosts |
| 993  | media.dyson.com               | 23.223.45.209  |  |  |  |
|      | brute_hosts |
| 994  | memphis.dyson.com             | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 995  | memphis.dyson.com             | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 996  | midwest.dyson.com             | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 997  | midwest.dyson.com             | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 998  | mh.dyson.com                  | 52.59.122.122  |  |  |  |
|      | brute_hosts |
| 999  | mh.dyson.com                  | 52.59.125.242  |  |  |  |
|      | brute_hosts |
| 1000 | milwaukee.dyson.com           | 52.59.122.122  |  |  |  |
|      | brute_hosts |
```

```
+-------+-----------------+-----------------+-----------+-----------+-----------+
|       | brute_hosts |
| 1930  | ye.dyson.com    | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1931  | ye.dyson.com    | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1932  | zeus.dyson.com  | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1933  | zeus.dyson.com  | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1934  | zlog.dyson.com  | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1935  | zlog.dyson.com  | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1936  | zm.dyson.com    | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1937  | zm.dyson.com    | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1938  | x.dyson.com     | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1939  | x.dyson.com     | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1940  | xml.dyson.com   | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1941  | xml.dyson.com   | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1942  | win1.dyson.com  | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1943  | win1.dyson.com  | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1944  | zebra.dyson.com | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1945  | zebra.dyson.com | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1946  | ws.dyson.com    | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1947  | ws.dyson.com    | 52.59.125.242   |           |           |           |
|       | brute_hosts |
| 1948  | zw.dyson.com    | 52.59.122.122   |           |           |           |
|       | brute_hosts |
| 1949  | zw.dyson.com    | 52.59.125.242   |           |           |           |
|       | brute_hosts |
+-------+-----------------+-----------------+-----------+-----------+-----------+

[*] 1949 rows returned
[recon-ng][test][brute_hosts] >
```

Crt.sh

It is also used to find subdomains. Then I created a file called subdomain.txt which contain all the subdomains when I found.

crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'dyson.com'

Sorry, your search results have been truncated.
It is not currently possible to sort and paginate large result sets efficiently, so only a random subset is shown below.
Please retry your search with expired certificates excluded.

Certificates

crt.sh ID	Logged At ↑	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5634142352	2021-11-18	2021-11-18	2022-12-17	api.cpdev002.dyson.com	api.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5633907480	2021-11-18	2021-11-18	2022-12-17	api.cpdev002.dyson.com	api.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5632957918	2021-11-18	2021-11-18	2022-12-17	staging2.shop.kr.dyson.com	staging2.shop.kr.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5632954246	2021-11-18	2021-11-18	2022-12-17	staging2.admin.shop.kr.dyson.com	staging2.admin.shop.kr.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5632575138	2021-11-18	2021-11-18	2022-12-17	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfmachinegw.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5631975283	2021-11-18	2021-11-18	2022-12-17	api.cpdev002.dyson.com	api.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5626723643	2021-11-17	2021-11-17	2022-10-30	*.dyson.com	*.dyson.com dyson.com qtest-staging.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5625987657	2021-11-17	2021-11-17	2022-12-16	api.cp.dyson.com	api.cp.dyson.com cfmachinegw.cp.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5625421558	2021-11-17	2021-11-17	2022-12-16	api.cpppe.dyson.com	api.cpppe.dyson.com cfmachinegw.cpppe.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5622756688	2021-11-17	2021-11-17	2022-12-15	*.dyson.cloud	*.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5622661187	2021-11-17	2021-10-12	2022-10-30	*.dyson.com	avsg.dyson.com *.dyson.com dyson.com sfbsg.dyson.com sip.dyson.com webconfsg.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5620809900	2021-11-16	2021-11-16	2022-12-15	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfmachinegw.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5620453663	2021-11-16	2021-11-16	2022-12-15	api.cpdev002.dyson.com	api.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5618996672	2021-11-16	2021-11-16	2022-12-17	staging-demo3D.dyson.com	staging-demo3D.dyson.com www.staging-demo3D.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5618989062	2021-11-16	2021-11-16	2022-12-17	demo3D.dyson.com	demo3D.dyson.com www.demo3D.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5615467934	2021-11-16	2021-11-16	2022-12-14	identity-hub.dyson.com	identity-hub.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5613340926	2021-11-15	2021-11-15	2022-12-14	api.cpsi.dyson.com	api.cpsi.dyson.com cfmachinegw.cpsi.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5613308673	2021-11-15	2021-11-15	2022-12-14	api.cpci.dyson.com	api.cpci.dyson.com cfmachinegw.cpci.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5612945113	2021-11-15	2021-11-15	2022-12-14	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfmachinegw.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5612764626	2021-11-15	2021-11-15	2022-12-14	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5612524469	2021-11-15	2021-11-15	2022-12-14	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfmachinegw.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5611777033	2021-11-15	2021-11-15	2022-12-14	api.cpsi.dyson.com	api.cpsi.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5611645086	2021-11-15	2021-11-15	2022-12-14	api.cpci.dyson.com	api.cpci.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5606072146	2021-11-14	2021-09-20	2021-12-19	gtm.dyson.com	gtm.dyson.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5603311429	2021-11-14	2021-11-14	2022-12-13	sslcertificate4.queue-it.net	queue.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5603121392	2021-11-14	2021-11-14	2022-12-13	sslcertificate4.queue-it.net	queue.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5600373561	2021-11-14	2021-11-14	2022-12-12	provisioningstatus.c3.cpdev003.dyson.com	provisioningstatus.c3.cpdev003.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592283662	2021-11-12	2021-11-12	2022-12-11	console.cpdev000.dyson.com	console.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592283694	2021-11-12	2021-11-12	2022-12-11	statuspage.cpdev000.dyson.com	statuspage.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592282278	2021-11-12	2021-11-12	2022-12-11	appapi.cpdev000.dyson.com	appapi.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592282103	2021-11-12	2021-11-12	2022-12-11	qr.cpdev000.dyson.com	qr.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592282302	2021-11-12	2021-11-12	2022-12-11	partnerapi.cpdev000.dyson.com	partnerapi.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592282208	2021-11-12	2021-11-12	2022-12-11	api.cpdev000.dyson.com	api.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592195513	2021-11-12	2021-11-12	2022-12-11	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592113766	2021-11-12	2021-11-12	2022-12-11	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5592016506	2021-11-12	2021-09-24	2022-10-14	*.dyson.com	*.dyson.com dyson.com s2pc.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5591667220	2021-11-12	2021-11-12	2022-12-11	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfmachinegw.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5591565813	2021-11-12	2021-11-12	2022-12-11	appapi.cpdev000.dyson.com	appapi.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5591565113	2021-11-12	2021-11-12	2022-12-11	qr.cpdev000.dyson.com	qr.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5591564921	2021-11-12	2021-11-12	2022-12-11	api.cpdev000.dyson.com	api.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5591564564	2021-11-12	2021-11-12	2022-12-11	partnerapi.cpdev000.dyson.com	partnerapi.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5591564516	2021-11-12	2021-11-12	2022-12-11	console.cpdev000.dyson.com	console.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5591564189	2021-11-12	2021-11-12	2022-12-11	statuspage.cpdev000.dyson.com	statuspage.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5590792348	2021-11-12	2021-11-12	2022-03-10	www.dyson.ie	admin.sa.dyson.com admin.shop.dyson.com.sg admin.shop.kr.dyson.com api-alexa-login.dyson.com api.dyson.com api.fi.dyson.com api-machine.dyson.com auth.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

					cfalbgwapi.cpdev002.dyson.com	
5578885893	2021-11-10	2021-11-10	2022-12-09	albgwapi.cpdev002.dyson.com	albgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5578637935	2021-11-10	2021-11-10	2022-12-09	statuspage.cpdev000.dyson.com	statuspage.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5578633817	2021-11-10	2021-11-10	2022-12-09	appapi.cpdev000.dyson.com	appapi.cpdev000.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5573467705	2021-11-09	2021-10-26	2022-11-23	betatrial.dyson.com	betatrial.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5573467682	2021-11-09	2021-10-06	2022-11-06	snow-gateway.dyson.com	snow-gateway.dyson.com www.snow-gateway.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5573467734	2021-11-09	2021-10-21	2022-10-30	*.dyson.com	*.dyson.com dyson.com idp-test.dyson.com idp-test-help.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5573467737	2021-11-09	2021-10-06	2022-10-30	*.dyson.com	*.dyson.com dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5572669915	2021-11-09	2021-11-09	2022-12-08	auth.cp.dyson.com	auth.cp.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572670002	2021-11-09	2021-11-09	2022-12-07	auth.cp.dyson.com	auth.cp.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572448197	2021-11-09	2021-11-09	2022-12-08	auth.cpppe.dyson.com	auth.cpppe.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572448033	2021-11-09	2021-11-09	2022-12-07	auth.cpppe.dyson.com	auth.cpppe.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572253811	2021-11-09	2021-11-09	2022-12-10	staging-demo3D.dyson.com	staging-demo3D.dyson.com www.staging-demo3D.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5572246411	2021-11-09	2021-11-09	2022-12-10	demo3D.dyson.com	demo3D.dyson.com www.demo3D.dyson.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
5572201628	2021-11-09	2021-11-09	2022-12-07	auth.cpsi.dyson.com	auth.cpsi.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572201413	2021-11-09	2021-11-09	2022-12-08	auth.cpsi.dyson.com	auth.cpsi.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572086785	2021-11-09	2021-11-09	2022-12-08	auth.cpci.dyson.com	auth.cpci.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5572086812	2021-11-09	2021-11-09	2022-12-07	auth.cpci.dyson.com	auth.cpci.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5567678962	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5567572529	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5567490182	2021-11-08	2021-11-08	2022-12-06	auth.cpdev003.dyson.com	auth.cpdev003.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5567488132	2021-11-08	2021-11-08	2022-12-07	auth.cpdev003.dyson.com	auth.cpdev003.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5567355132	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5567226727	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5566933937	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5566642484	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5566504547	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5565849233	2021-11-08	2021-11-08	2022-12-07	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5550063113	2021-11-05	2021-11-05	2022-12-04	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5549751795	2021-11-05	2021-11-05	2022-12-04	api.cpdev002.dyson.com	api.cpdev002.dyson.com cfalbgwapi.cpdev002.dyson.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon

Here I consider more about the following sub-domain because those are the most important for organizations.

%api%
%corp%
%internal%

Then I have found more interesting sub dominos and I include all these to subdomain.txt

Alive sub domains

Httprobe

httprobe is a tool commonly used in penetration testing and security assessments. It is used to probe a list of domain names and identify which ones are accessible via HTTP or HTTPS.

Here is how it generally works:

1. You provide httprobe with a list of domain names.

2. httprobe sends HTTP or HTTPS requests to each domain.

3. It records which domains respond with valid HTTP responses, indicating that they are "alive" and accessible.

This tool can be useful for identifying active web servers within a target domain or for verifying the accessibility of a list of domains.

- To install httprob
  $ sudo apt install httprobe

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ sudo apt install httprobe
[sudo] password for rasan:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  httprobe
0 upgraded, 1 newly installed, 0 to remove and 1886 not upgraded.
Need to get 1,597 kB of archives.
After this operation, 4,653 kB of additional disk space will be used.
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 httprobe amd64 0.2-0kali1 [1,597 kB]
Fetched 1,597 kB in 5s (327 kB/s)
Selecting previously unselected package httprobe.
(Reading database ... 397676 files and directories currently installed.)
Preparing to unpack .../httprobe_0.2-0kali1_amd64.deb ...
Unpacking httprobe (0.2-0kali1) ...
Setting up httprobe (0.2-0kali1) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for kali-menu (2023.2.3) ...
```

- I have saved subdomain.txt file in my Dekstop
  $ cat subdomain.txt|httprobe >> live.txt

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ cat subdomain.txt|httprobe >> live.txt

┌──(rasan㉿kali)-[~/Desktop]
└─$ cat live.txt
http://loadtest.dyson.com
http://lyncdiscoverinternal.dyson.com
http://lyncweb.dyson.com
https://media.dyson.com
http://oneview.dyson.com
http://media.dyson.com
http://webconf.dyson.com
http://webmail-jp.dyson.com
http://webmail-sg.dyson.com
http://webmail-us.dyson.com
http://adminservice.dyson.com
http://akamai.dyson.com
http://adminqaservice.dyson.com
http://origin.akamai.dyson.com
https://api-alexa-login.dyson.com
https://www.ar.dyson.com
http://av.dyson.com
http://api-alexa-login.dyson.com
http://www.ar.dyson.com
http://avus.dyson.com
https://beta.dyson.com
https://authoring.b2bapp.dyson.com
http://beta.dyson.com
http://authoring.b2bapp.dyson.com
http://build.dyson.com
https://careers.dyson.com
https://business.dyson.com
http://careers.dyson.com
https://www.careers.dyson.com
http://business.dyson.com
http://www.careers.dyson.com
https://central.dyson.com
https://www.central.dyson.com
http://autodiscover.dyson.com
http://av-sg.dyson.com
http://cheetah-cn.dyson.com
http://cheetah-uk.dyson.com
https://cmcontroltower.dyson.com
http://cheetah-au.dyson.com
http://cheetah-us.dyson.com
http://www.community.dyson.com
http://cmcontroltower.dyson.com
http://gwr.perf.connected.dyson.com
http://gwr.ppe.connected.dyson.com
http://gwr.prd.connected.dyson.com
http://gwr.si.connected.dyson.com
https://community.dyson.com
http://community.dyson.com
```

http://lyncdiscoverinternal.dyson.com
http://loadtest.dyson.com
http://lyncweb.dyson.com
https://media.dyson.com
http://media.dyson.com
http://webmail-sg.dyson.com
http://webconf.dyson.com
http://webmail-us.dyson.com
http://oneview.dyson.com
http://webmail-jp.dyson.com
http://adminservice.dyson.com
http://adminqaservice.dyson.com
http://origin.akamai.dyson.com
http://akamai.dyson.com
https://www.ar.dyson.com
https://api-alexa-login.dyson.com
http://www.ar.dyson.com
http://av-sg.dyson.com
http://api-alexa-login.dyson.com
https://authoring.b2bapp.dyson.com
http://authoring.b2bapp.dyson.com
https://beta.dyson.com
http://beta.dyson.com
http://build.dyson.com
http://av.dyson.com
https://careers.dyson.com
http://careers.dyson.com
http://avus.dyson.com
https://www.careers.dyson.com
http://www.careers.dyson.com
https://central.dyson.com
https://www.central.dyson.com
http://autodiscover.dyson.com
http://cheetah-au.dyson.com
http://cheetah-jp.dyson.com
http://console.cp.dyson.com
http://cheetah-cn.dyson.com
http://cheetah-uk.dyson.com
https://business.dyson.com
http://www.community.dyson.com
https://cmcontroltower.dyson.com
http://business.dyson.com
https://community.dyson.com
http://gwr.perf.connected.dyson.com
http://cmcontroltower.dyson.com
http://community.dyson.com
http://gwr.prd.connected.dyson.com
http://gwr.ppe.connected.dyson.com
http://gwr.si.connected.dyson.com
http://cheetah-sg.dyson.com
http://cheetah-us.dyson.com
http://www.communit.dyson.com
https://api.cp.dyson.com
http://api.cp.dyson.com
https://appapi.cp.dyson.com
http://communit.dyson.com
http://appapi.cp.dyson.com
https://cost-calculator.dyson.com
https://contentfi.dyson.com
https://auth.cp.dyson.com
http://cost-calculator.dyson.com
https://content.dyson.com
http://auth.cp.dyson.com
http://content.dyson.com
http://contentfi.dyson.com
https://console.cp.dyson.com
http://commvault-test.dyson.com
http://gwr.stg.connected.dyson.com
https://partnerapi.cp.dyson.com
https://qr.cp.dyson.com
https://statuspage.cp.dyson.com
https://gwr.cp.dyson.com

https://interapi.cp.dyson.com
http://gwr.uat.connected.dyson.com
http://partnerapi.cp.dyson.com
http://qr.cp.dyson.com
http://statuspage.cp.dyson.com
https://appapi.cpci.dyson.com
https://auth.cpci.dyson.com
http://connectedgwr.dyson.com
http://appapi.cpci.dyson.com
http://auth.cpci.dyson.com
https://gwr.cpci.dyson.com
https://interapi.cpci.dyson.com
https://console.cpci.dyson.com
https://partnerapi.cpci.dyson.com
http://console.cpci.dyson.com
http://partnerapi.cpci.dyson.com
https://statuspage.cpci.dyson.com
https://qr.cpci.dyson.com
https://api.cpci.dyson.com
http://statuspage.cpci.dyson.com
http://qr.cpci.dyson.com
http://api.cpci.dyson.com
https://appapi.cpcommon-dev.dyson.com
https://console.cpcommon-dev.dyson.com
https://partnerapi.cpcommon-dev.dyson.com
https://appapi.cpdev000.dyson.com
https://auth.cpdev000.dyson.com
https://console.cpdev000.dyson.com
https://partnerapi.cpdev000.dyson.com
https://statuspage.cpdev000.dyson.com
https://gwr.cpdev000.dyson.com
https://appapi.cpdev001.dyson.com
https://auth.cpdev001.dyson.com
https://console.cpdev001.dyson.com
https://idpm.cpdev001.dyson.com
http://gwr.cpdev.dyson.com
https://partnerapi.cpdev001.dyson.com
https://api.cpdev002.dyson.com
https://appapi.cpdev002.dyson.com
http://api.cpdev002.dyson.com
https://auth.cpdev002.dyson.com
http://appapi.cpdev002.dyson.com
http://auth.cpdev002.dyson.com
https://console.cpdev002.dyson.com
http://console.cpdev002.dyson.com
https://qr.cpdev002.dyson.com
https://statuspage.cpdev002.dyson.com
http://qr.cpdev002.dyson.com
https://partnerapi.cpdev002.dyson.com
http://statuspage.cpdev002.dyson.com
http://partnerapi.cpdev002.dyson.com
https://appapi.cpdev003.dyson.com
https://console.cpdev003.dyson.com
https://auth.cpdev003.dyson.com
https://gwr.cpdev003.dyson.com
https://interapi.cpdev003.dyson.com
https://partnerapi.cpdev003.dyson.com
https://qr.cpdev003.dyson.com
https://appapi.cpdev004.dyson.com
https://partnerapi.cpdev004.dyson.com
https://interapi.cpdev004.dyson.com
https://idpm.cpdev004.dyson.com

https://statuspage.cpdev004.dyson.com
https://appapi.cpeqdev.dyson.com
https://console.cpeqdev.dyson.com
http://partnerapi.cpimgclass-prd.dyson.com
http://api.cplt.dyson.com
http://appapi.cplt.dyson.com
http://cfappapi.cplt.dyson.com
http://gwr.cplt.dyson.com
https://appapi.cpmldev.dyson.com
https://console.cpmldev.dyson.com
https://partnerapi.cpmldev.dyson.com
https://statuspage.cpmldev.dyson.com
http://appapi.cpimgclass-dev.dyson.com
http://partnerapi.cpimgclass-dev.dyson.com
http://agappapi.cppe.dyson.com
http://api.cpimgclass-prd.dyson.com
http://agcfappapi.cppe.dyson.com
http://appapi.cppe.dyson.com
https://api.cpppe.dyson.com
http://gwr.cpperf.dyson.com
https://interapi.cppki-dev.dyson.com
http://appapi.cpimgclass-prd.dyson.com
https://appapi.cpppe.dyson.com
http://api.cpppe.dyson.com
https://auth.cpppe.dyson.com
https://interapi.cppki-prd.dyson.com
http://agappapi.cplt.dyson.com
http://agcfappapi.cplt.dyson.com
http://appapi.cpppe.dyson.com
http://auth.cpppe.dyson.com
http://partnerapi.cplt.dyson.com
https://console.cpdev004.dyson.com
https://partnerapi.cpeqdev.dyson.com
http://api.cpimgclass-dev.dyson.com

https://console.cpppe.dyson.com
http://gwr.cplt2.dyson.com
https://interapi.cpppe.dyson.com
https://gwr.cpppe.dyson.com
https://partnerapi.cpppe.dyson.com
https://qr.cpppe.dyson.com
http://partnerapi.cplt2.dyson.com
https://statuspage.cpppe.dyson.com
http://console.cpppe.dyson.com
http://partnerapi.cpppe.dyson.com
http://qr.cpppe.dyson.com
https://api.cpsi.dyson.com
http://statuspage.cpppe.dyson.com
https://appapi.cpsi.dyson.com
https://auth.cpsi.dyson.com
http://api.cpsi.dyson.com
http://appapi.cpsi.dyson.com
http://auth.cpsi.dyson.com
http://cfappapi.cppe.dyson.com
https://console.cpsi.dyson.com
https://partnerapi.cpsi.dyson.com
http://console.cpsi.dyson.com
https://statuspage.cpsi.dyson.com
http://partnerapi.cpsi.dyson.com
https://qr.cpsi.dyson.com
http://statuspage.cpsi.dyson.com
http://qr.cpsi.dyson.com
https://interapi.cpsi.dyson.com
https://gwr.cpsi.dyson.com
http://partnerapi.cpsileap.dyson.com
http://api.cpstage.dyson.com
http://appapi.cpstage.dyson.com

http://auth.cpstage.dyson.com
http://launcher.c3.cpstage.dyson.com
http://srg.c3.cpstage.dyson.com
http://dsr.c3.cpstage.dyson.com
http://cfqr.cpstage.dyson.com
http://partnerapi.cpqa.dyson.com
http://partnerapi.cpstage.dyson.com
http://qr.cpstage.dyson.com
http://gwr.cpqa.dyson.com
http://gwr.cpsileap.dyson.com
http://cpstage.dyson.com
http://gwr.cpstage.dyson.com
http://n276-eb1-trial.cpstage.dyson.com
http://gwr.cptrials.dyson.com
http://gwr.cptest.dyson.com
http://agcfappapi.cpuat.dyson.com
http://cfappapi.cpuat.dyson.com
http://partnerapi.cpuat.dyson.com
http://daybook.dyson.com
https://demo3d.dyson.com
http://demo3d.dyson.com
http://deu-lt02.dyson.com
http://desktop-my.dyson.com
http://agappapi.cpuat.dyson.com
http://appapi.cpuat.dyson.com
http://gwr.cpuat.dyson.com
http://desktop-sea.dyson.com
http://devices.dyson.com
http://dialin.dyson.com
https://dysoncmg.dyson.com
https://click.e.dyson.com
http://click.e.dyson.com
https://cloud.e.dyson.com
http://cloud.e.dyson.com
https://view.e.dyson.com
http://ota.c3.cpstage.dyson.com
http://cfappapi.cpstage.dyson.com
http://view.e.dyson.com
https://image.e.dyson.com
http://image.e.dyson.com
http://epm.dyson.com
http://epm-test.dyson.com
https://feedback.dyson.com
http://feedback.dyson.com
https://beta.fi.dyson.com
https://shop.fi.dyson.com
http://beta.fi.dyson.com
http://shop.fi.dyson.com
http://gbr-lt02.dyson.com
https://api.fi.dyson.com
https://www.forbusiness-preferences.dyson.com
http://api.fi.dyson.com
http://www.forbusiness-preferences.dyson.com
https://www.gr.dyson.com
http://www.gr.dyson.com
https://gtm.dyson.com
http://gtm.dyson.com
https://identity-hub.dyson.com
http://idp-help.dyson.com
http://identity-hub.dyson.com
http://ircpp.dyson.com
http://www.isseymiyake.dyson.com
http://idp-test-help.dyson.com
https://kr.dyson.com
http://kr.dyson.com
https://registration.kr.dyson.com
http://registration.kr.dyson.com
https://admin.shop.kr.dyson.com
http://www.krefel.dyson.com

https://landscape.dyson.com
https://staging.shop.kr.dyson.com
http://jpn-lt02.dyson.com
https://staging.admin.shop.kr.dyson.co
m
http://admin.shop.kr.dyson.com
http://landscape.dyson.com
https://www.kz.dyson.com
http://staging.admin.shop.kr.dyson.co
m
http://staging.shop.kr.dyson.com
http://www.kz.dyson.com
https://www.lb.dyson.com
https://support.kr.dyson.com
https://linkapp-api.dyson.com
http://www.lb.dyson.com
http://support.kr.dyson.com
http://lync.dyson.com
http://linkapp-api.dyson.com
http://learning.dyson.com
http://linkserver-api.dyson.com
http://loadtest.dyson.com
http://lyncweb.dyson.com
http://lyncweb-us.dyson.com
http://local-test.dyson.com
http://lyncdiscoverinternal.dyson.com
http://lyncweb-sg.dyson.com
https://media.dyson.com
http://lyncweb-my.dyson.com
http://media.dyson.com
http://meet.dyson.com
http://motor-test.dyson.com
http://officewa-uk-test.dyson.com
http://oneview.dyson.com
https://oldmedia.dyson.com
http://oldmedia.dyson.com
https://privacy.dyson.com
http://privacy.dyson.com
http://project-test.dyson.com
https://queue.dyson.com
http://queue.dyson.com
https://remote-rvd.dyson.com
https://remote-vdi.dyson.com
http://qtest-staging.dyson.com
http://reviews.dyson.com
https://www.sa.dyson.com
http://s2pc.dyson.com
http://s4herpcs01c.dyson.com
http://s4hq44app01v.dyson.com
http://www.s4hq44app01v.dyson.com
https://staging.sa.dyson.com
https://forbusiness.sa.dyson.com
http://sa.dyson.com
https://saa.dyson.com
https://admin.sa.dyson.com
http://www.sa.dyson.com
https://support.sa.dyson.com
http://staging.sa.dyson.com
http://forbusiness.sa.dyson.com
http://saa.dyson.com
http://admin.sa.dyson.com
http://support.sa.dyson.com
https://staging.admin.sa.dyson.com
http://staging.admin.sa.dyson.com
http://www.s4herpcs01c.dyson.com
http://sccscpapp01v.dyson.com
http://www.sccscnapp01v.dyson.com
http://wildcard.san.dyson.com
http://sccscnapp01v.dyson.com
http://www.sccscpapp01v.dyson.com
http://service.dyson.com
http://sea.dyson.com

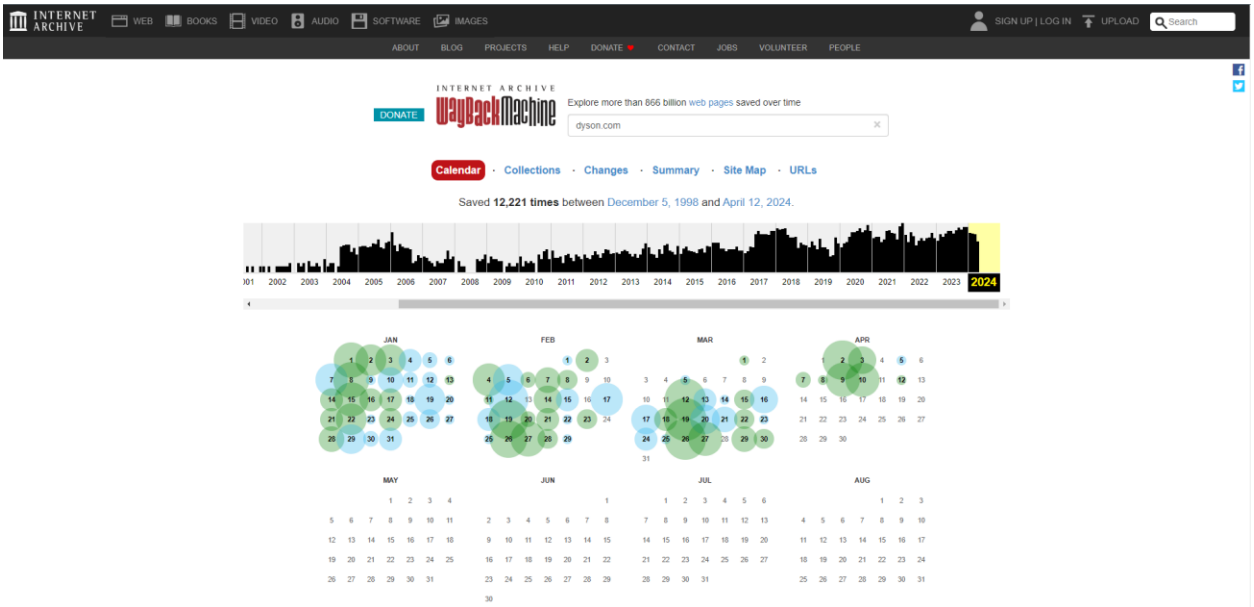
http://selfresolve.dyson.com
http://sipus.dyson.com
https://snow-gateway.dyson.com
https://staging-demo3d.dyson.com
https://tableau.dyson.com
http://staging-demo3d.dyson.com
http://skypewebus.dyson.com
http://tableau.dyson.com
https://tandcs.dyson.com
https://teamcentermy.dyson.com
https://teamcentersg.dyson.com
https://teamcenteruk.dyson.com
http://tandcs.dyson.com
http://teamcentermy.dyson.com
https://teamcenteruk-dev.dyson.com
http://teamcentersg.dyson.com
https://telescope.dyson.com
http://tableauchina.dyson.com
http://tableaudev.dyson.com
http://teamcenteruk.dyson.com
http://tableauqas.dyson.com
http://teamcenteruk-dev.dyson.com
http://test.dyson.com
http://uk-mal-ise-adm.dyson.com
http://www.uk-mal-ise-adm.dyson.com
http://uk-mal-ise-adm-01.dyson.com
http://webconf.dyson.com
http://teamcenter.dyson.com
http://webconfus.dyson.com
http://webconf-sg.dyson.com
http://webmail-au.dyson.com
http://webmail-us.dyson.com
http://webmaildr.dyson.com
http://webmailtest.dyson.com
http://xyz.dyson.com
http://webmail.dyson.com
http://www.webmail.dyson.com
http://webmail-jp.dyson.com
http://webmail-my.dyson.com
http://webmail-sg.dyson.com

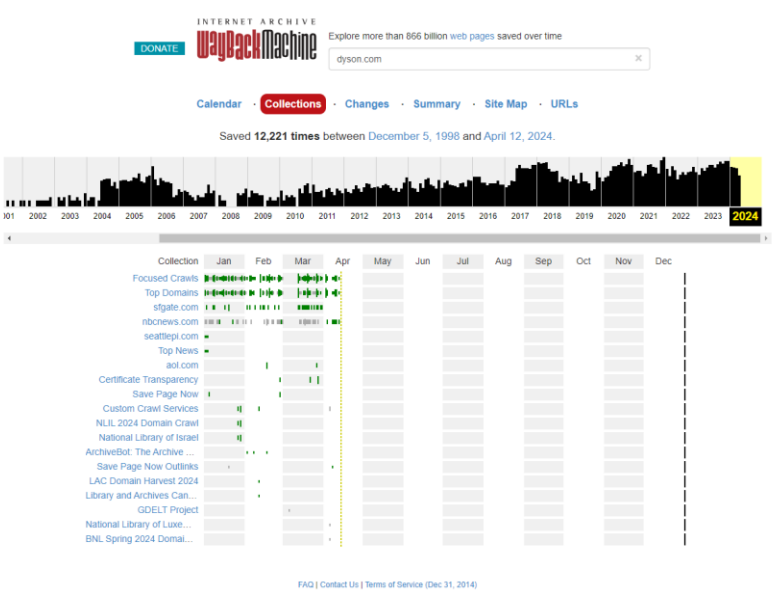
Find Archived information.

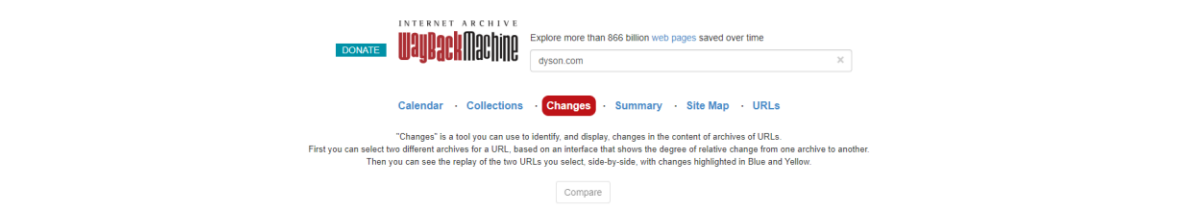
Wayback machine

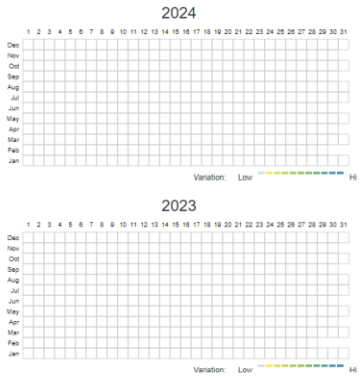
Website link - https://web.archive.org/web

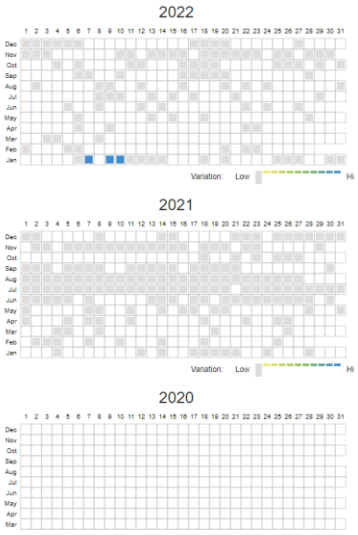
The Wayback Machine is a digital archive of the World Wide Web maintained by the Internet Archive a nonprofit organization. It allows users to access archived versions of web pages over time essentially providing a historical snapshot of the internet.

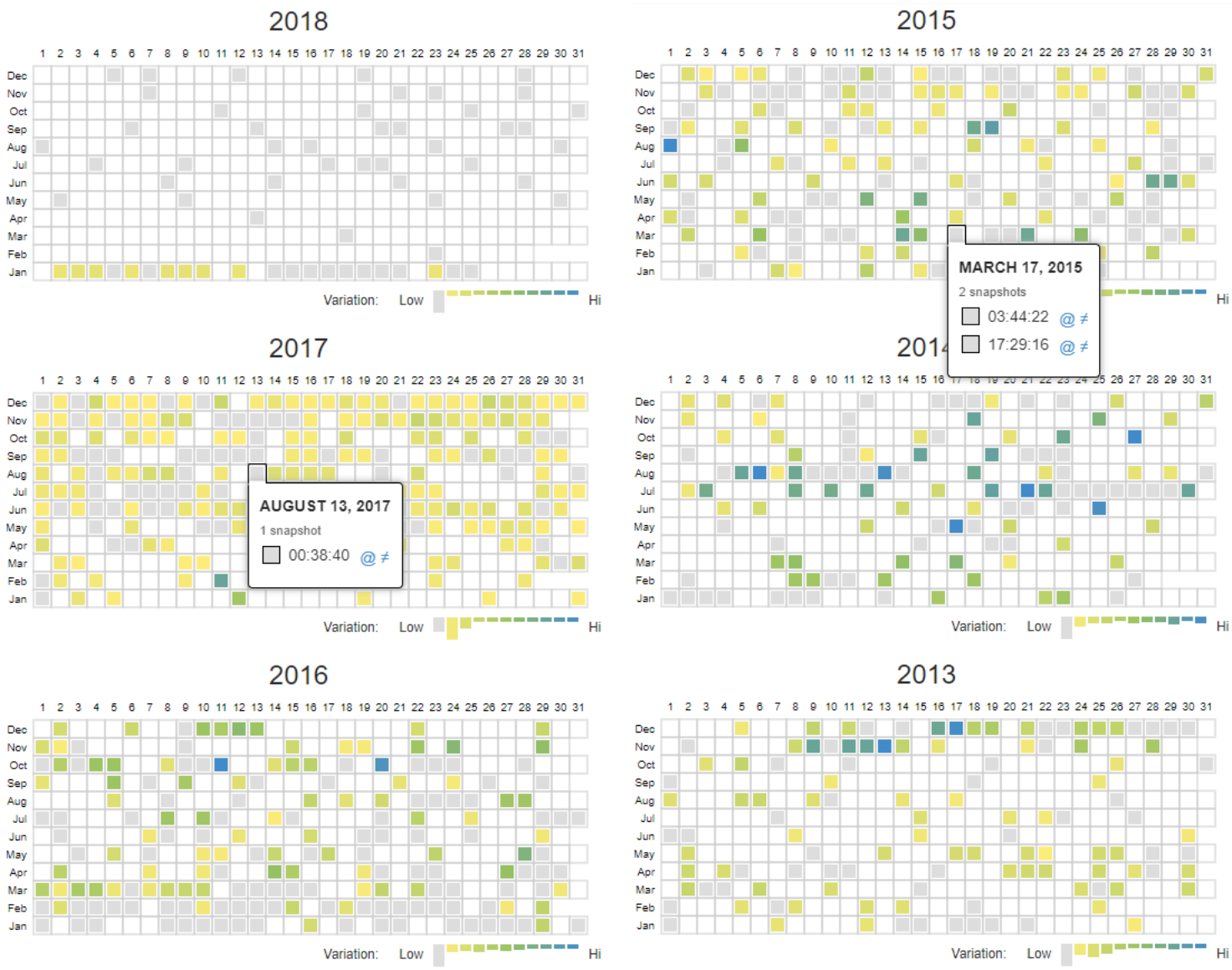


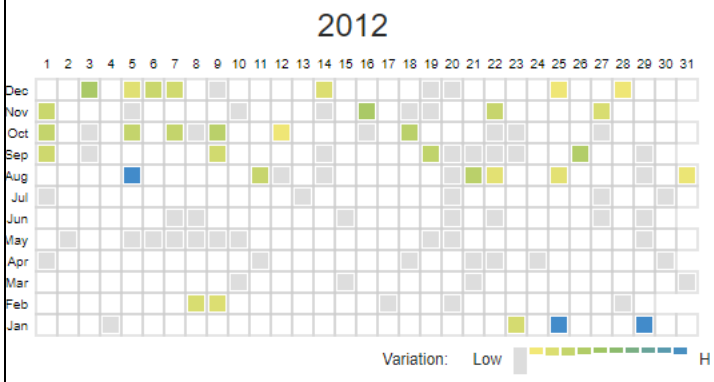

INTERNET ARCHIVE
DONATE
WayBackMachine
Explore more than 866 billion web pages saved over time
dyson.com
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 12,221 times between December 5, 1998 and April 12, 2024.
2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024
Collection Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Focused Crawls
Top Domains
sfgate.com
nbcnews.com
seattlepi.com
Top News
aol.com
Certificate Transparency
Save Page Now
Custom Crawl Services
NLIL 2024 Domain Crawl
National Library of Israel
ArchiveBot: The Archive ...
Save Page Now Outlinks
LAC Domain Harvest 2024
Library and Archives Can...
GDELT Project
National Library of Luxe...
BNL Spring 2024 Domai...
FAQ | Contact Us | Terms of Service (Dec 31, 2014)

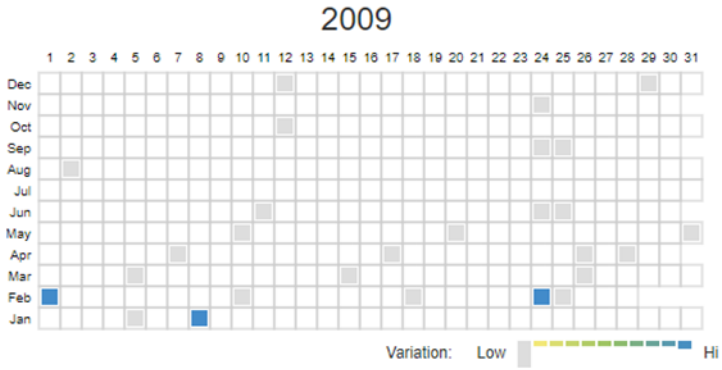

INTERNET ARCHIVE
DONATE
WayBackMachine
Explore more than 866 billion web pages saved over time
dyson.com
Calendar · Collections · Changes · Summary · Site Map · URLs
"Changes" is a tool you can use to identify, and display, changes in the content of archives of URLs.
First you can select two different archives for a URL, based on an interface that shows the degree of relative change from one archive to another.
Then you can see the replay of the two URLs you select, side-by-side, with changes highlighted in Blue and Yellow.
Compare

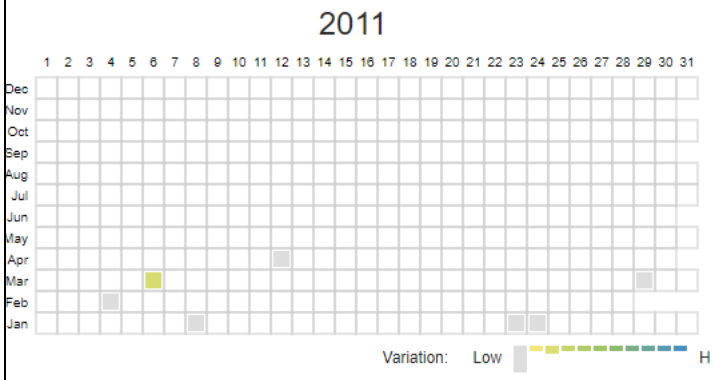

2024
Variation: Low
2023
Variation: Low

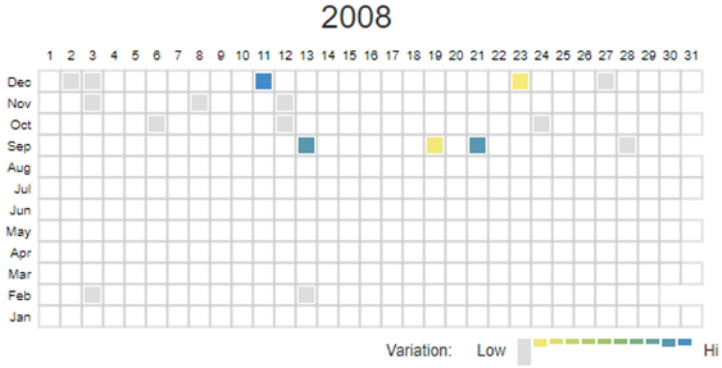

2022
2021
2020
Variation: Low

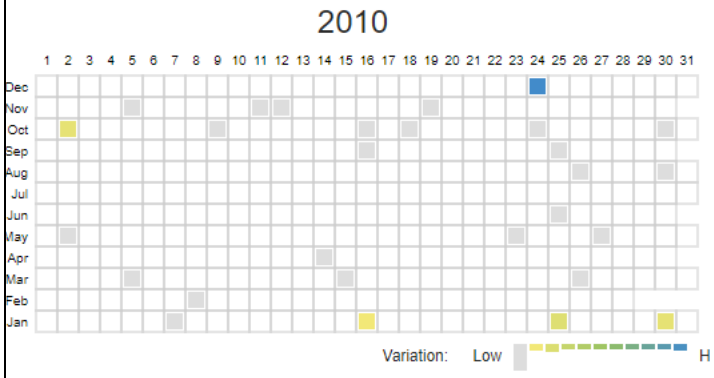

2018
2015
MARCH 17, 2015
2 snapshots
03:44:22
17:29:16
2017
AUGUST 13, 2017
1 snapshot
00:38:40
2014
2016
2013
Variation: Low Hi

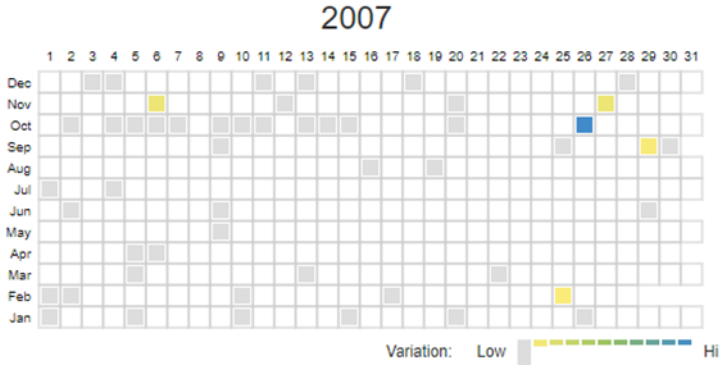

2012
Variation: Low H


2009
Variation: Low Hi


2011
Variation: Low H


2008
Variation: Low Hi


2010
Variation: Low H


2007
Variation: Low Hi

This is very helpful for information gathering because we can find some interesting data with this process. Such as,

- Old forgotten endpoints
- Interesting JS files
- Sensitive information

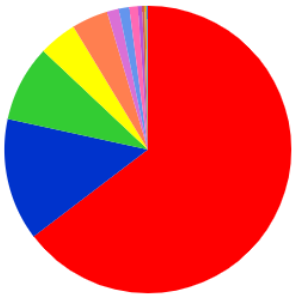
Summary on MIME-types Count

Quick search on MIME-types...

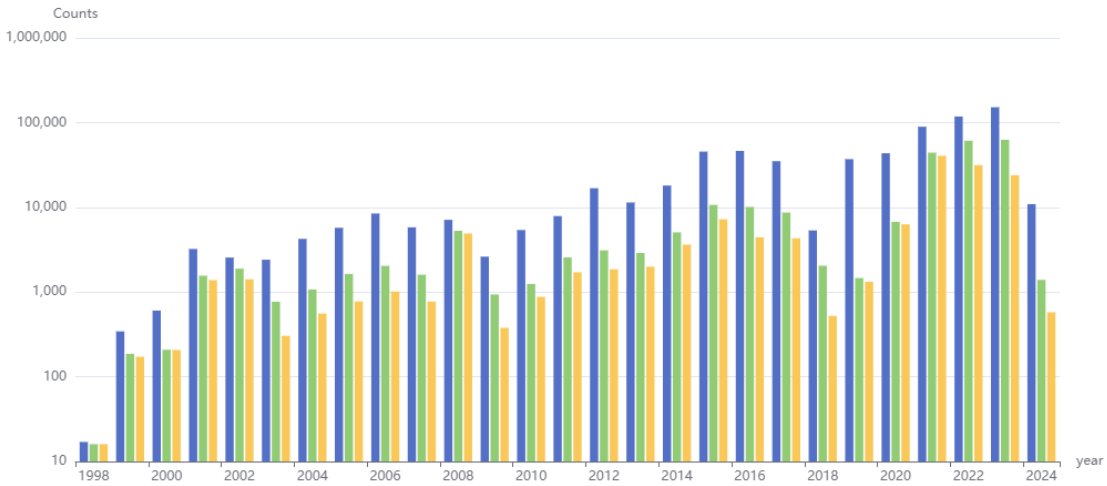
<< < 1 2 ... > >>

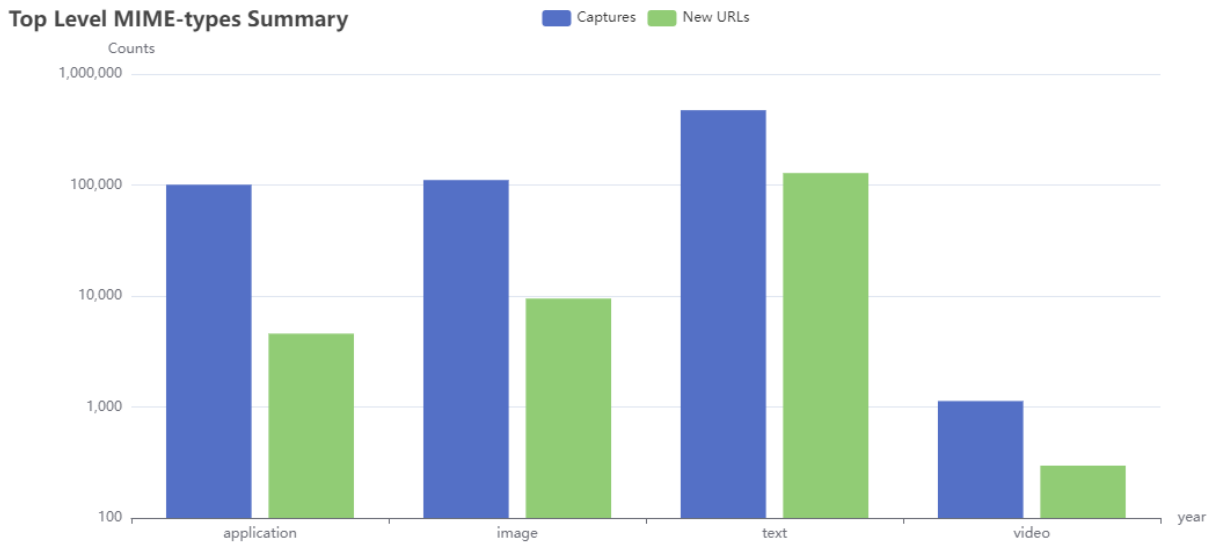
	Captures	Unique URLs
text/html	442,746	125,765
application/javascript	94,206	3,200
image/png	58,846	1,514
text/css	29,422	2,339
image/jpeg	28,029	6,975
image/gif	9,128	972
image/svg+xml	8,134	17
image/vnd.microsoft.icon	6,681	1
application/json	3,212	195
application/pdf	1,899	948

Captures



Keys Summary For the TLD/Host/Domain





Last 10 Captures

Capture	Statuscode	MIME-type	Size (bytes)
Fri, 12 Apr 2024 04:43:07 GMT	301	text/html	1,353
Wed, 10 Apr 2024 08:32:04 GMT	301	text/html	1,396
Wed, 10 Apr 2024 08:31:54 GMT	301	unk	1,179
Wed, 10 Apr 2024 08:10:07 GMT	301	text/html	1,396
Wed, 10 Apr 2024 08:10:00 GMT	301	unk	1,176
Wed, 10 Apr 2024 07:02:49 GMT	301	text/html	483
Wed, 10 Apr 2024 06:21:17 GMT	301	text/html	1,213
Wed, 10 Apr 2024 06:21:10 GMT	301	unk	1,177
Wed, 10 Apr 2024 05:01:47 GMT	301	text/html	481
Wed, 10 Apr 2024 03:51:22 GMT	301	text/html	1,411

Summery

Moreover URLS

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://dyson.com/.well-known/ai-plugin.json	text/html	Jul 12, 2023	Jul 13, 2023	2	0	2
http://dyson.com/.well-known/assetlinks.json	text/html	Jul 12, 2023	Jul 12, 2023	1	0	1
http://dyson.com/.well-known/dnt-policy.txt	text/html	Jul 12, 2023	Jul 13, 2023	2	0	2
http://dyson.com/.well-known/gpc.json	text/html	Jul 12, 2023	Jul 13, 2023	3	1	2
http://dyson.com/.well-known/nodeinfo	text/html	Jul 12, 2023	Jul 13, 2023	3	1	2
http://dyson.com/.well-known/openid-configuration	text/html	Jul 12, 2023	Jul 13, 2023	2	0	2
http://dyson.com/.well-known/security.txt	text/html	Jul 12, 2023	Jul 13, 2023	3	1	2
http://dyson.com/.well-known/trust.txt	text/html	Jul 12, 2023	Jul 13, 2023	3	1	2
http://dyson.com/547-global-qr	text/html	Jan 15, 2023	Jan 15, 2023	1	0	1
http://dyson.com/674-global-qr	text/html	Jul 23, 2022	Jul 23, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=J4JP3c6gpvc&ranSiteID=J4JP3c6gpvc-6k.EApC.bxeTF_qcSVIPKg&siteID=J4JP3c6gpvc-6k.EApC.bxeTF_qcSVIPKg&utm_source=sepascartagena.org&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 5, 2022	Mar 5, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=J4JP3c6gpvc&ranSiteID=J4JP3c6gpvc-pqPwb6z2WlKfqiD6Muwt4g&siteID=J4JP3c6gpvc-pqPwb6z2WlKfqiD6Muwt4g&utm_source=sepascartagena.org&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 4, 2022	Mar 4, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=J4JP3c6gpvc&ranSiteID=J4JP3c6gpvc-QYHLeIBFYKGIU7KtXyKm7Q&siteID=J4JP3c6gpvc-QYHLeIBFYKGIU7KtXyKm7Q&utm_source=sepascartagena.org&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 2, 2022	Mar 2, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-0gIYoaQ57Y0pfaKz0YBsdQ&siteID=je6NUbpObpQ-0gIYoaQ57Y0pfaKz0YBsdQ	text/html	Feb 2, 2021	Feb 11, 2021	6	5	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-0gIYoaQ57Y0pfaKz0YBsdQ&siteID=je6NUbpObpQ-0gIYoaQ57Y0pfaKz0YBsdQ&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 2, 2021	Feb 2, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-_WVKm_RaEAjjKAIP8qQVKA&siteID=je6NUbpObpQ-_WVKm_RaEAjjKAIP8qQVKA	text/html	Feb 1, 2021	Feb 14, 2021	5	4	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-_WVKm_RaEAjjKAIP8qQVKA&siteID=je6NUbpObpQ-_WVKm_RaEAjjKAIP8qQVKA&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 1, 2021	Feb 1, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-dv3WZWGfwXjPhu5HhPCwpQ&siteID=je6NUbpObpQ-dv3WZWGfwXjPhu5HhPCwpQ	text/html	Feb 5, 2021	Feb 23, 2021	3	2	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-dv3WZWGfwXjPhu5HhPCwpQ&siteID=je6NUbpObpQ-dv3WZWGfwXjPhu5HhPCwpQ&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 5, 2021	Feb 5, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-fVxTDoKiTAcaevhtDpaQrg&siteID=je6NUbpObpQ-fVxTDoKiTAcaevhtDpaQrg	text/html	Feb 14, 2021	Mar 4, 2021	3	2	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-fVxTDoKiTAcaevhtDpaQrg&siteID=je6NUbpObpQ-fVxTDoKiTAcaevhtDpaQrg&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 11, 2021	Feb 11, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-G3pPPtvOlDth33yc9.JM0A&siteID=je6NUbpObpQ-G3pPPtvOlDth33yc9.JM0A	text/html	Feb 8, 2021	Feb 28, 2021	5	4	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-G3pPPtvOlDth33yc9.JM0A&siteID=je6NUbpObpQ-G3pPPtvOlDth33yc9.JM0A&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 8, 2021	Feb 8, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-HMbOlzUCbF5Alx2y3bgsGQ&siteID=je6NUbpObpQ-HMbOlzUCbF5Alx2y3bgsGQ	text/html	Feb 4, 2021	Feb 8, 2021	4	3	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-HMbOlzUCbF5Alx2y3bgsGQ&siteID=je6NUbpObpQ-HMbOlzUCbF5Alx2y3bgsGQ&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 4, 2021	Feb 4, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-OHHw0Gbolrt4UDasS7tYFQ&siteID=je6NUbpObpQ-OHHw0Gbolrt4UDasS7tYFQ	text/html	Jan 30, 2021	Feb 12, 2021	7	6	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-OHHw0Gbolrt4UDasS7tYFQ&siteID=je6NUbpObpQ-OHHw0Gbolrt4UDasS7tYFQ&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Jan 30, 2021	Jan 30, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-yqzbiPSJzmEjuMl0GPAm8A&siteID=je6NUbpObpQ-yqzbiPSJzmEjuMl0GPAm8A&utm_source=VigLink&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Feb 14, 2021	Feb 14, 2021	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=pITOEqOhvpQ&ranSiteID=pITOEqOhvpQ-ReSqH4I1q0brGXP3tWlkw&siteID=pITOEqOhvpQ-ReSqH4I1q0brGXP3tWlkw&utm_source=Brandreward&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Dec 6, 2023	Dec 6, 2023	2	0	2
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rlmY&ranSiteID=tv2R4u9rlmY-993wYvH0vvwUlkVnDOpg_A&siteID=tv2R4u9rlmY-993wYvH0vvwUlkVnDOpg_A&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 20, 2022	Mar 20, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rlmY&ranSiteID=tv2R4u9rlmY-fw2S8xa2wmlv6nrjs2SQUQ&siteID=tv2R4u9rlmY-fw2S8xa2wmlv6nrjs2SQUQ&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Apr 4, 2021	Apr 5, 2021	2	0	2
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rlmY&ranSiteID=tv2R4u9rlmY-j2aOv3.oubBdnBVfkcQE8g&siteID=tv2R4u9rlmY-j2aOv3.oubBdnBVfkcQE8g&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 20, 2022	Mar 20, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rlmY&ranSiteID=tv2R4u9rlmY-sKIZrdj1gMveA8R0oaecZw&siteID=tv2R4u9rlmY-sKIZrdj1gMveA8R0oaecZw&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Oct 25, 2022	Oct 26, 2022	2	0	2
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rlmY&ranSiteID=tv2R4u9rlmY-VSH1szXY4Oo2diumtDI8NA&siteID=tv2R4u9rlmY-VSH1szXY4Oo2diumtDI8NA&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 20, 2022	Mar 20, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rlmY&ranSiteID=tv2R4u9rlmY-yhYZdl7TYm9xOxB42toZAQ&siteID=tv2R4u9rlmY-yhYZdl7TYm9xOxB42toZAQ&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 19, 2022	Mar 19, 2022	1	0	1

http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rImY&ranSiteID=tv2R4u9rImY-sKIZrdj1gMveA8R0oaecZw&siteID=tv2R4u9rImY-sKIZrdj1gMveA8R0oaecZw&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Oct 25, 2022	Oct 26, 2022	2	0	2
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rImY&ranSiteID=tv2R4u9rImY-VSH1szXY4Oo2diumtDI8NA&siteID=tv2R4u9rImY-VSH1szXY4Oo2diumtDI8NA&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 20, 2022	Mar 20, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=tv2R4u9rImY&ranSiteID=tv2R4u9rImY-yhYZdl7TYm9xOxB42toZAQ&siteID=tv2R4u9rImY-yhYZdl7TYm9xOxB42toZAQ&utm_source=Skimlinks+(Variable+Pricing)&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Mar 19, 2022	Mar 19, 2022	1	0	1
http://dyson.com/?ranMID=36310&ranEAID=ucE5BarM2zo&ranSiteID=ucE5BarM2zo-2AtyJECBybRfdcXvIO04rg&siteID=ucE5BarM2zo-2AtyJECBybRfdcXvIO04rg&utm_source=TODAY+Show&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Jul 12, 2022	Jul 12, 2022	3	1	2
http://dyson.com/?ranMID=36310&ranEAID=ucE5BarM2zo&ranSiteID=ucE5BarM2zo-y8hXokvQPprG4DjVXW7ATw&siteID=ucE5BarM2zo-y8hXokvQPprG4DjVXW7ATw&utm_source=TODAY+Show&utm_medium=affiliate&utm_campaign=us_en__na__na__na__purchase&utm_term=&utm_content=rakuten_1	text/html	Jul 16, 2022	Jul 16, 2022	2	0	2
http://dyson.com/?utm_source=Page_&utm_medium=o_social&utm_campaign=EC_support_always-on_&utm_content=care_own-social_twitter_help_me_solve_100003199227753_20220626__&utm_term=Customer_Care%3A_Agents_Canada	text/html	Jul 14, 2022	Jul 14, 2022	1	0	1
http://dyson.com/?utm_source=Twitter_N%2FA&utm_medium=o_social&utm_campaign=N%2FA_support_always-on_&utm_content=care_own-social_twitter_help_me_solve__&utm_term=Customer_Care%3A_Agents_Canada	text/html	Nov 23, 2020	Feb 12, 2021	22	21	1
http://dyson.com/addmyattachment	text/html	Jan 19, 2021	Feb 11, 2021	11	10	1
http://dyson.com/aftersales/images/handheld.jpg	text/html	Mar 16, 2013	Mar 29, 2013	2	1	1
http://dyson.com/aftersales/images/upright.jpg	text/html	Mar 16, 2013	Mar 16, 2013	1	0	1
http://dyson.com/air-treatment/air-puri...	text/html	Nov 22, 2021	Nov 16, 2022	5	3	2
http://dyson.com/airwrap-accessoriesからお問い合わせください。	text/html	Dec 27, 2022	Dec 27, 2022	1	0	1
http://dyson.com/airwrap-accessoriesからお問い合わせください。本製品についてAirwrap™カーラー	text/html	Dec 27, 2022	Dec 27, 2022	1	0	1
http://dyson.com:80/88i9tmfR48ievLOYciloQ==	text/html	Feb 24, 2009	Feb 24, 2009	1	0	1
http://dyson.com:80/about/ads/?movie=ball_principles_us	text/html	Jan 30, 2009	Apr 18, 2012	4	0	4
http://dyson.com:80/about/ads/?movie=DC24_product_ad	text/html	Jan 30, 2009	Apr 18, 2012	9	1	8
http://dyson.com:80/aftersales/help.asp?article_id=32&hist=,,1	text/html	Oct 13, 2007	Nov 4, 2007	2	0	2
http://dyson.com:80/aftersales/help.asp?showOption=1&path_id=1&article_id=1&hist=,,1	text/html	Oct 13, 2007	Oct 13, 2007	1	0	1

Wayback URLs

Wayback gives a list of all the URLs that the wayback Machine known about for a domain.

Git link - https://github.com/tomnomnom/waybackurls

First, we want to install it.

$ go install github.com/tomnomnom/waybackurls@latest

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ go install github.com/tomnomnom/waybackurls@latest
Command 'go' not found, but can be installed with:
sudo apt install gccgo-go
sudo apt install golang-go
```

In here go command is not found therefor we want to install it.

$ sudo apt install golang-go

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ sudo apt install golang-go

[sudo] password for rasan:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  golang-1.22-go golang-1.22-src golang-src libpkgconf3 pkg-config pkgconf pkgconf-bin
Suggested packages:
  bzr | brz mercurial
The following NEW packages will be installed:
  golang-1.22-go golang-1.22-src golang-go golang-src libpkgconf3 pkg-config pkgconf pkgconf-bin
0 upgraded, 8 newly installed, 0 to remove and 1886 not upgraded.
Need to get 43.7 MB of archives.
After this operation, 228 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:6 http://http.kali.org/kali kali-rolling/main amd64 pkgconf-bin amd64 1.8.1-1+b2 [29.7 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libpkgconf3 amd64 1.8.1-1+b2 [36.4 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 golang-1.22-go amd64 1.22.2-1 [24.7 MB]
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 golang-1.22-src all 1.22.2-1 [18.8 MB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 golang-src all 2:1.22~3 [5,020 B]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 pkgconf amd64 1.8.1-1+b2 [26.2 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 pkg-config amd64 1.8.1-1+b2 [14.0 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 golang-go amd64 2:1.22~3 [44.2 kB]
Fetched 43.7 MB in 10s (4,181 kB/s)
Selecting previously unselected package golang-1.22-src.
(Reading database ... 397682 files and directories currently installed.)
Preparing to unpack .../0-golang-1.22-src_1.22.2-1_all.deb ...
Unpacking golang-1.22-src (1.22.2-1) ...
Selecting previously unselected package golang-1.22-go.
Preparing to unpack .../1-golang-1.22-go_1.22.2-1_amd64.deb ...
Unpacking golang-1.22-go (1.22.2-1) ...
Selecting previously unselected package golang-src.
Preparing to unpack .../2-golang-src_2%3a1.22~3_all.deb ...
```

Now we can install the wayback url

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ go install github.com/tomnomnom/waybackurls@latest
go: downloading github.com/tomnomnom/waybackurls v0.1.0
```

It is done.

I get all the archived urls of the dyson domain by sending the alive domains through the waybackurls and save as urls.txt

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ cat live.txt | waybackurls > urls
waybackurls: command not found
```

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ cat urls.txt
http://loadtest.dyson.com
http://lyncdiscoverinternal.dyson.com
http://lyncweb.dyson.com
https://media.dyson.com
http://oneview.dyson.com
http://media.dyson.com
http://webconf.dyson.com
http://webmail-jp.dyson.com
http://webmail-sg.dyson.com
http://webmail-us.dyson.com
http://adminservice.dyson.com
http://akamai.dyson.com
http://adminqaservice.dyson.com
http://origin.akamai.dyson.com
https://api-alexa-login.dyson.com
https://www.ar.dyson.com
http://av.dyson.com
http://api-alexa-login.dyson.com
http://www.ar.dyson.com
http://avus.dyson.com
https://beta.dyson.com
https://authoring.b2bapp.dyson.com
http://beta.dyson.com
http://authoring.b2bapp.dyson.com
http://build.dyson.com
https://careers.dyson.com
https://business.dyson.com
http://careers.dyson.com
https://www.careers.dyson.com
http://business.dyson.com
http://www.careers.dyson.com
https://central.dyson.com
https://www.central.dyson.com
http://autodiscover.dyson.com
http://av-sg.dyson.com
http://cheetah-cn.dyson.com
http://cheetah-uk.dyson.com
https://cmcontroltower.dyson.com
http://cheetah-au.dyson.com
http://cheetah-us.dyson.com
http://www.community.dyson.com
http://cmcontroltower.dyson.com
http://gwr.perf.connected.dyson.com
http://gwr.ppe.connected.dyson.com
http://gwr.prd.connected.dyson.com
http://gwr.si.connected.dyson.com
https://community.dyson.com
http://community.dyson.com
https://content.dyson.com
http://content.dyson.com
https://cost-calculator.dyson.com
```

```
http://connectedgwr.dyson.com
http://gwr.uat.connected.dyson.com
http://qr.cpci.dyson.com
http://statuspage.cpci.dyson.com
http://communit.dyson.com
https://gwr.cpci.dyson.com
https://interapi.cpci.dyson.com
https://appapi.cpcommon-dev.dyson.com
https://console.cpcommon-dev.dyson.com
https://partnerapi.cpcommon-dev.dyson.com
http://gwr.cpdev.dyson.com
https://appapi.cpdev000.dyson.com
https://auth.cpdev000.dyson.com
https://console.cpdev000.dyson.com
https://gwr.cpdev000.dyson.com
https://partnerapi.cpdev000.dyson.com
https://statuspage.cpdev000.dyson.com
https://appapi.cpdev001.dyson.com
https://auth.cpdev001.dyson.com
https://idpm.cpdev001.dyson.com
https://console.cpdev001.dyson.com
https://partnerapi.cpdev001.dyson.com
https://api.cpdev002.dyson.com
https://appapi.cpdev002.dyson.com
https://auth.cpdev002.dyson.com
http://api.cpdev002.dyson.com
http://appapi.cpdev002.dyson.com
https://console.cpdev002.dyson.com
http://auth.cpdev002.dyson.com
https://partnerapi.cpdev002.dyson.com
http://console.cpdev002.dyson.com
https://qr.cpdev002.dyson.com
https://statuspage.cpdev002.dyson.com
http://partnerapi.cpdev002.dyson.com
http://qr.cpdev002.dyson.com
http://statuspage.cpdev002.dyson.com
https://auth.cpdev003.dyson.com
https://console.cpdev003.dyson.com
https://appapi.cpdev003.dyson.com
https://gwr.cpdev003.dyson.com
https://interapi.cpdev003.dyson.com
https://partnerapi.cpdev003.dyson.com
https://qr.cpdev003.dyson.com
https://appapi.cpdev004.dyson.com
https://idpm.cpdev004.dyson.com
https://console.cpdev004.dyson.com
https://interapi.cpdev004.dyson.com
https://partnerapi.cpdev004.dyson.com
https://statuspage.cpdev004.dyson.com
https://console.cpeqdev.dyson.com
https://appapi.cpeqdev.dyson.com
https://partnerapi.cpeqdev.dyson.com
http://api.cpimgclass-prd.dyson.com
```

```
http://auth.cpppe.dyson.com
http://gwr.cplt.dyson.com
http://gwr.cplt2.dyson.com
http://partnerapi.cplt2.dyson.com
http://cfappapi.cppe.dyson.com
http://appapi.cppe.dyson.com
https://console.cpppe.dyson.com
http://console.cpppe.dyson.com
https://partnerapi.cpppe.dyson.com
http://partnerapi.cpppe.dyson.com
https://gwr.cpppe.dyson.com
https://statuspage.cpppe.dyson.com
https://interapi.cpppe.dyson.com
http://statuspage.cpppe.dyson.com
https://qr.cpppe.dyson.com
https://api.cpsi.dyson.com
https://appapi.cpsi.dyson.com
http://qr.cpppe.dyson.com
http://api.cpsi.dyson.com
http://appapi.cpsi.dyson.com
https://auth.cpsi.dyson.com
http://auth.cpsi.dyson.com
http://gwr.cpqa.dyson.com
https://partnerapi.cpsi.dyson.com
http://partnerapi.cpsi.dyson.com
https://qr.cpsi.dyson.com
http://qr.cpsi.dyson.com
https://interapi.cpsi.dyson.com
https://gwr.cpsi.dyson.com
https://console.cpsi.dyson.com
https://statuspage.cpsi.dyson.com
http://console.cpsi.dyson.com
http://statuspage.cpsi.dyson.com
http://gwr.cpsileap.dyson.com
http://partnerapi.cpqa.dyson.com
http://cpstage.dyson.com
http://partnerapi.cpsileap.dyson.com
http://api.cpstage.dyson.com
http://appapi.cpstage.dyson.com
http://auth.cpstage.dyson.com
http://ota.c3.cpstage.dyson.com
http://dsr.c3.cpstage.dyson.com
http://cfqr.cpstage.dyson.com
http://cfappapi.cpstage.dyson.com
http://gwr.cpstage.dyson.com
http://n276-eb1-trial.cpstage.dyson.com
http://launcher.c3.cpstage.dyson.com
http://srg.c3.cpstage.dyson.com
http://partnerapi.cpstage.dyson.com
http://appapi.cpuat.dyson.com
http://qr.cpstage.dyson.com
http://gwr.cptest.dyson.com
http://partnerapi.cpuat.dyson.com
```

```
http://view.e.dyson.com
https://image.e.dyson.com
http://image.e.dyson.com
http://epm-test.dyson.com
http://epm.dyson.com
https://feedback.dyson.com
http://feedback.dyson.com
https://api.fi.dyson.com
http://api.fi.dyson.com
https://beta.fi.dyson.com
http://beta.fi.dyson.com
https://shop.fi.dyson.com
http://shop.fi.dyson.com
https://www.forbusiness-preferences.dyson.com
http://www.forbusiness-preferences.dyson.com
http://gbr-lt02.dyson.com
https://gtm.dyson.com
https://www.gr.dyson.com
http://gtm.dyson.com
http://www.gr.dyson.com
https://identity-hub.dyson.com
http://identity-hub.dyson.com
http://idp-help.dyson.com
http://ircpp.dyson.com
http://www.isseymiyake.dyson.com
http://jpn-lt02.dyson.com
https://kr.dyson.com
http://kr.dyson.com
http://idp-test-help.dyson.com
https://registration.kr.dyson.com
http://registration.kr.dyson.com
https://admin.shop.kr.dyson.com
http://admin.shop.kr.dyson.com
http://www.krefel.dyson.com
https://staging.admin.shop.kr.dyson.com
http://staging.admin.shop.kr.dyson.com
https://support.kr.dyson.com
https://staging.shop.kr.dyson.com
http://support.kr.dyson.com
https://landscape.dyson.com
http://staging.shop.kr.dyson.com
https://www.lb.dyson.com
http://www.lb.dyson.com
http://landscape.dyson.com
http://linkserver-api.dyson.com
http://loadtest.dyson.com
https://linkapp-api.dyson.com
https://www.kz.dyson.com
http://www.kz.dyson.com
http://linkapp-api.dyson.com
http://local-test.dyson.com
http://lync.dyson.com
http://lyncdiscoverinternal.dyson.com
```

DNS Enumeration

DNSrecon

dnsrecon is a powerful DNS enumeration tool used by security professionals and system administrators to gather information about a target domain in DNS infrastructure. It can help identify DNS records, subdomains and other DNS-related information which can be useful for reconnaissance and security assessments.

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ dnsrecon -h
usage: dnsrecon [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b]
                [-y] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB]
                [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion]
                [--disable_check_bindversion] [-V] [-v] [-t TYPE]

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the target will be use
d. Multiple servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats   (first-last) or in (
range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for brute force.
  -f                    Filter out of brute force domain lookup, records that resolve to the wild
card defined IP address when saving records.
  -a                    Perform AXFR with standard enumeration.
  -s                    Perform a reverse lookup of IPv4 ranges in the SPF record with standard e
numeration.
  -b                    Perform Bing enumeration with standard enumeration.
  -y                    Perform Yandex enumeration with standard enumeration.
  -k                    Perform crt.sh enumeration with standard enumeration.
  -w                    Perform deep whois record analysis and reverse lookup of IP ranges found
through Whois when doing a standard enumeration.
  -z                    Performs a DNSSEC zone walk with standard enumeration.
  --threads THREADS     Number of threads to use in reverse lookups, forward lookups, brute force
 and SRV record enumeration.
  --lifetime LIFETIME   Time to wait for a server to respond to a query. default is 3.0
  --tcp                 Use TCP protocol to make queries.
  --db DB               SQLite 3 file to save found records.
  -x XML, --xml XML     XML file to save found records.
  -c CSV, --csv CSV     Save output to a comma separated value file.
  -j JSON, --json JSON  save output to a JSON file.
  --iw                  Continue brute forcing a domain even if a wildcard record is discovered.
  --disable_check_recursion
                        Disables check for recursion on name servers
  --disable_check_bindversion
                        Disables check for BIND version on name servers
  -V, --version         Show DNSrecon version
  -v, --verbose         Enable verbose
  -t TYPE, --type TYPE  Type of enumeration to perform.
                        Possible types:
                            std:      SOA, NS, A, AAAA, MX and SRV.
                            rvl:      Reverse lookup of a given CIDR or IP range.
```

```
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the target will be use
d. Multiple servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats   (first-last) or in (
range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for brute force.
  -f                    Filter out of brute force domain lookup, records that resolve to the wild
card defined IP address when saving records.
  -a                    Perform AXFR with standard enumeration.
  -s                    Perform a reverse lookup of IPv4 ranges in the SPF record with standard e
numeration.
  -b                    Perform Bing enumeration with standard enumeration.
  -y                    Perform Yandex enumeration with standard enumeration.
  -k                    Perform crt.sh enumeration with standard enumeration.
  -w                    Perform deep whois record analysis and reverse lookup of IP ranges found
through Whois when doing a standard enumeration.
  -z                    Performs a DNSSEC zone walk with standard enumeration.
  --threads THREADS     Number of threads to use in reverse lookups, forward lookups, brute force
 and SRV record enumeration.
  --lifetime LIFETIME   Time to wait for a server to respond to a query. default is 3.0
  --tcp                 Use TCP protocol to make queries.
  --db DB               SQLite 3 file to save found records.
  -x XML, --xml XML     XML file to save found records.
  -c CSV, --csv CSV     Save output to a comma separated value file.
  -j JSON, --json JSON  save output to a JSON file.
  --iw                  Continue brute forcing a domain even if a wildcard record is discovered.
  --disable_check_recursion
                        Disables check for recursion on name servers
  --disable_check_bindversion
                        Disables check for BIND version on name servers
  -V, --version         Show DNSrecon version
  -v, --verbose         Enable verbose
  -t TYPE, --type TYPE  Type of enumeration to perform.
                        Possible types:
                            std:      SOA, NS, A, AAAA, MX and SRV.
                            rvl:      Reverse lookup of a given CIDR or IP range.
                            brt:      Brute force domains and hosts using a given dictionary.
                            srv:      SRV records.
                            axfr:     Test all NS servers for a zone transfer.
                            bing:     Perform Bing search for subdomains and hosts.
                            yand:     Perform Yandex search for subdomains and hosts.
                            crt:      Perform crt.sh search for subdomains and hosts.
                            snoop:    Perform cache snooping against all NS servers for a given d
omain, testing
                                      all with file containing the domains, file given with -D op
tion.

                            tld:      Remove the TLD of given domain and test against all TLDs re
gistered in IANA.
                            zonewalk: Perform a DNSSEC zone walk using NSEC records.
```

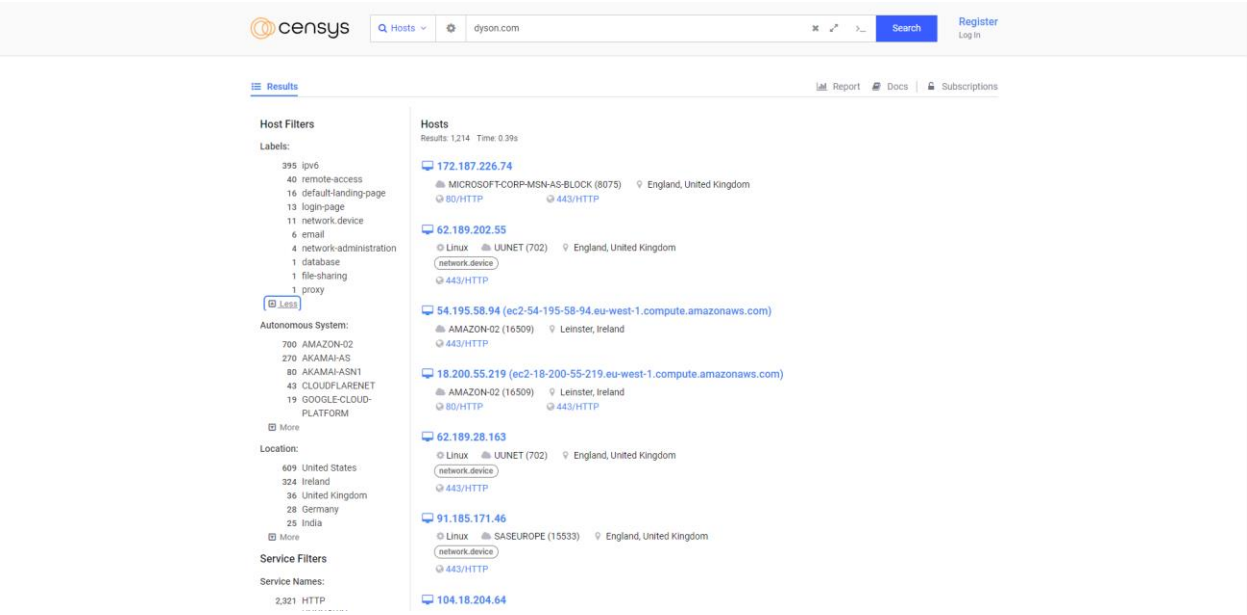
```
┌──(rasan㉿kali)-[~/Desktop]
└─$ dnsrecon -d dyson.com -D /usr/share/wordlists/dnsmao.txt -t std --xml dnsrecon.xml
[*] std: Performing General Enumeration against: dyson.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 52.59.125.242
[!] It is resolving to 52.59.122.122
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for dyson.com
[*]      SOA a1-82.akam.net 193.108.91.82
[*]      SOA a1-82.akam.net 2600:1401:2::52
[*]      NS a24-65.akam.net 2.16.130.65
[*]      Bind Version for 2.16.130.65 "18706.35"
[*]      NS a24-65.akam.net 2600:1480:9800::41
[*]      NS a9-67.akam.net 184.85.248.67
[*]      Bind Version for 184.85.248.67 "45197.133"
[*]      NS a9-67.akam.net 2a02:26f0:117::43
[*]      NS a13-64.akam.net 2.22.230.64
[*]      Bind Version for 2.22.230.64 "17146.15"
[*]      NS a13-64.akam.net 2600:1480:800::40
[*]      NS a4-67.akam.net 72.246.46.67
[*]      Bind Version for 72.246.46.67 "16721.106"
[*]      NS a4-67.akam.net 2600:1480:9000::43
[*]      NS a2-65.akam.net 95.100.174.65
[*]      Bind Version for 95.100.174.65 "32153.14"
[*]      NS a2-65.akam.net 2600:1480:7000::41
[*]      NS a1-82.akam.net 193.108.91.82
[*]      Bind Version for 193.108.91.82 "33301.7"
[*]      NS a1-82.akam.net 2600:1401:2::52
[*]      MX cluster5a.eu.messagelabs.com 34.253.63.114
[*]      MX cluster6.eu.messagelabs.com 195.245.230.200
[*]      MX cluster6.eu.messagelabs.com 195.245.231.75
[*]      MX cluster6.eu.messagelabs.com 195.245.231.69
[*]      MX cluster6.eu.messagelabs.com 85.158.142.215
[*]      MX cluster6.eu.messagelabs.com 195.245.230.202
[*]      MX cluster6.eu.messagelabs.com 85.158.142.214
[*]      MX cluster6.eu.messagelabs.com 85.158.142.210
[*]      MX cluster6.eu.messagelabs.com 195.245.230.201
[*]      MX cluster5.eu.messagelabs.com 195.245.230.200
[*]      MX cluster5.eu.messagelabs.com 195.245.231.72
[*]      MX cluster5.eu.messagelabs.com 85.158.142.214
[*]      MX cluster5.eu.messagelabs.com 85.158.142.210
[*]      MX cluster5.eu.messagelabs.com 85.158.142.215
[*]      MX cluster5.eu.messagelabs.com 195.245.230.201
[*]      MX cluster5.eu.messagelabs.com 195.245.230.202
[*]      MX cluster5.eu.messagelabs.com 195.245.231.69
[*]      A dyson.com 52.59.125.242
[*]      A dyson.com 52.59.122.122
[*]      TXT dyson.com TLJpF41larFk9PJtq+o/Z5/krseHKw/MKYdUnS7jIt4JN8QB1Y70EQROrveMKYb3TkriTLQzfH
sP7XNVwrU/HA==
[*]      TXT dyson.com google-site-verification=TmH9r7e1J2DhO-vn1Ue1MAjK-Ab2SRlc_ayefgsPnDk
[*]      TXT dyson.com MS=ms77862664
[*]      TXT dyson.com atlassian-domain-verification=mHZCKzSjmA7wzVBGabVO7KuTC7myGMUGHD995GzUFemH
eygvtFuDKZfAbGe/yeEP
```

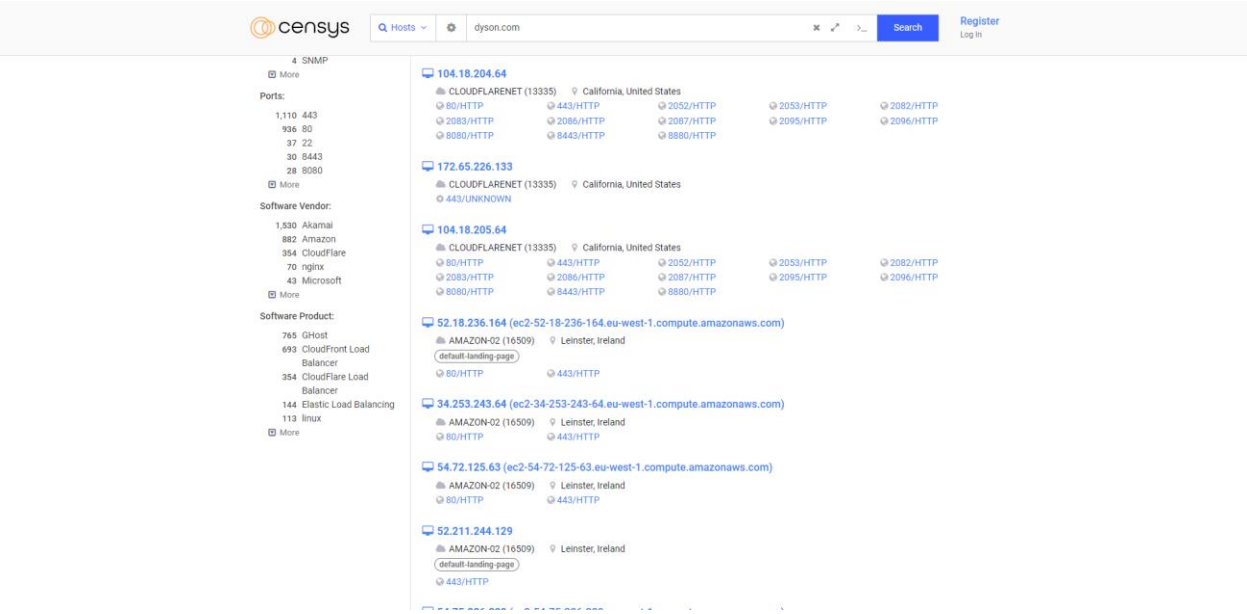
```
[*]     TXT dyson.com atlassian-domain-verification=mHZCKzSjmA7wzVBGabVO7KuTC7myGMUGHD995GzUFemH
eygvtFuDKZfAbGe/yeEP
[*]     TXT dyson.com f6fqqcst2ytjq9k6z60k8mdrtbtnc917
[*]     TXT dyson.com google-site-verification=XlX5gL0jGe87iiO2tULNOuRy-mo--pdckka19-42_CM
[*]     TXT dyson.com n9f9ffn5x5ccb31cqr8vqfj5n9f9d441
[*]     TXT dyson.com D0Y4S36957
[*]     TXT dyson.com atlassian-domain-verification=b4S+whRbLjHV52d9G88diHwrLSxwE+8fkBIzY1yXiI+p
uiwOILzLHTFD1hVmBHGI
[*]     TXT dyson.com _spf.salesforce.com
[*]     TXT dyson.com sending_domain707593=79d7217f4ec50b948a4ff0ffb4178e79b8b19e15845fb7c4e238e
b5844375b4b
[*]     TXT dyson.com google-site-verification=Z2nIWvQ0ZjSaVy0SjEvXbicqaRyTMCqCxzr7MqTiAoc
[*]     TXT dyson.com jm9099r0lfgrnsgby8jz6c5lws4csrrg
[*]     TXT dyson.com 2kxhnmlzm6pswtb9mdm9s53nnh06yd7m
[*]     TXT dyson.com onetrust-domain-verification=ba64ce248a3e4f1ea206304f9c89facb
[*]     TXT dyson.com pardot707593=1f9630953073bff2ff5cfb9a3216657c0218246795183417d51b8db0d139f
463
[*]     TXT dyson.com MS=ms85753066
[*]     TXT dyson.com tbn7rk9sl946lkl0x3nqnblvk1vj51nr
[*]     TXT dyson.com facebook-domain-verification=ni9lzurpvqhm6ss4vxy6imuskwrcen
[*]     TXT dyson.com 4zxp1vt1l6y0wck4ttbflxfcsk0blfs0
[*]     TXT dyson.com google-site-verification=XlgdeFq9Af0QStyvoETBmO2V6FeWetL5VagS13SGwdE
[*]     TXT dyson.com docusign=00733cd5-da40-4be9-95f0-df4641a6b42d
[*]     TXT dyson.com apple-domain-verification=x8SRPDt1TRupsgNt
[*]     TXT dyson.com have-i-been-pwned-verification=2eac33a3f09c8d6c48bd8514eff4f1fd
[*]     TXT dyson.com google-site-verification=DlvwXlWDQ8lxw0tZ_iT9-4sEwcs_S5VXf7CVux2Y8gk
[*]     TXT dyson.com tzkktsxtbg4px1bq20qd7bf6t2t5t15g
[*]     TXT dyson.com nxfz9jbyngpx9j9vw8ty6h5xgyx7k9fb
[*]     TXT dyson.com teamviewer-sso-verification=901cef60988c41dc88cd5df869100a54
[*]     TXT dyson.com google-site-verification=TjrbwsVnmHLwVHYodKC68ArJO7dmFtIfe5z6Pdl2z8I
[*]     TXT dyson.com nk83mwp5dh2chmcc15crblg3vhmm0n20
[*]     TXT dyson.com google-site-verification=_1a7SvndV-jf4PvimZDdRZ6Bm8ExDpXhYzxjXkBmo5s
[*]     TXT dyson.com facebook-domain-verification=kx2ehlffb6a9fus3rbzdf4wkxvqp47
[*]     TXT dyson.com onetrust-domain-verification=618aac7c48fc4376a762e092f6a2ce22
[*]     TXT dyson.com apple-domain-verification=7WyoAd3qpQseEmU8
[*]     TXT dyson.com wnxtjwmhyqmddr38x0y7x1s9h3tnzsjg
[*]     TXT dyson.com miro-verification=9fdefb52f2fa5c3a03902c3e7f1fd425842e71ff
[*]     TXT dyson.com google-site-verification=zJPB_uQEXTY7B7ZxHdsdHKTD8GWx7hKR0mPrxyGSVu8
[*]     TXT dyson.com v=spf1 include:%{i}._ip.%{h}._ehlo.%{d}._spf.emailfraudprotect.email ~all
[*]     TXT dyson.com onetrust-domain-verification=7392234825b144a08441475f7b6584ab
[*]     TXT dyson.com q9xkj7p3f6x8fdsr4h55mhbyxdq8sntq
[*]     TXT dyson.com K7ofhysb3YtvqJCmOB5IIUZzkPpIAsnOTaIvW5sdmrf/ijtUBWjtjAlgZwT7glxtgy4JQ/S9xl
hfMgu7Qg+rcQ==
[*]     TXT dyson.com adobe-idp-site-verification=96996838a96169031c6d7d8b55b781e1628ae0bc39393d
17ba75370e3070cdee
[*]     TXT _dmarc.dyson.com v=DMARC1; p=none; aspf=r; rua=mailto:dmarc_agg@emailfraudprotect.em
ail,mailto:dmarc_aggdata@dyson.com; ruf=mailto:dmarc_aggdata@dyson.com
[*] Enumerating SRV Records
[+]     SRV _sipfederationtls._tcp.dyson.com sipfed.online.lync.com 52.114.159.167 5061
[+] 1 Records Found
[*] Saving records to XML file: dnsrecon.xml
```

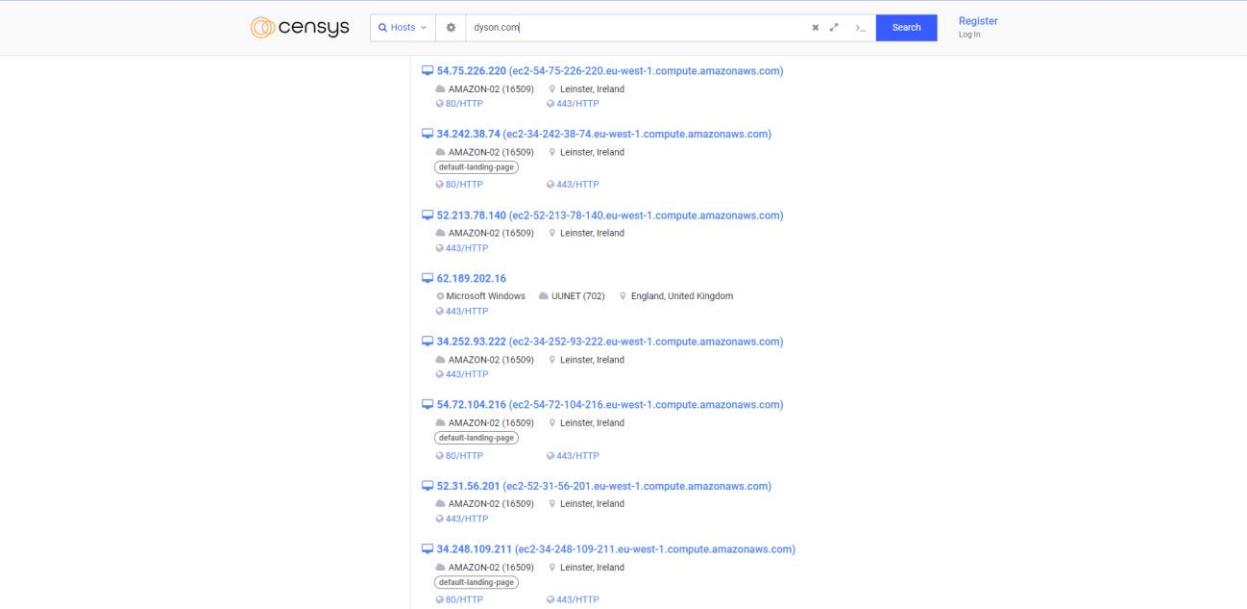
Public Device Enumeration

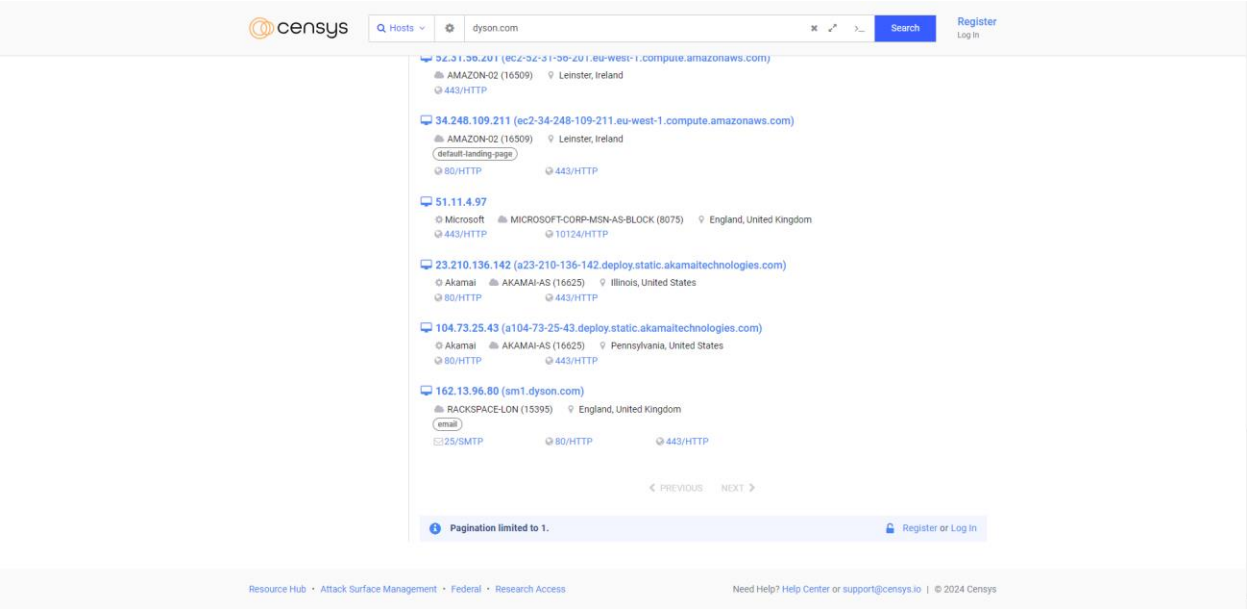
Censys

Censys is a valuable tool for gaining insights into internet infrastructure, identifying security risk, and monitoring the security posture of organizations and networks. However, it's important to use censys responsibly and in compliance with it is term of service and acceptable use policy.


censys
Hosts
dyson.com
Search
Register
Log In
Results
Report
Docs
Subscriptions
Host Filters
Labels:
395 ipv6
40 remote-access
16 default-landing-page
13 login-page
11 network.device
6 email
4 network-administration
1 database
1 file-sharing
1 proxy
Less
Autonomous System:
700 AMAZON-02
270 AKAMAI-AS
80 AKAMAI-ASN1
43 CLOUDFLARENET
19 GOOGLE-CLOUD-PLATFORM
More
Location:
609 United States
324 Ireland
36 United Kingdom
28 Germany
25 India
More
Service Filters
Service Names:
2,321 HTTP
Hosts
Results: 1,214 Time: 0.39s
172.187.226.74
MICROSOFT-CORP-MSN-AS-BLOCK (8075)
England, United Kingdom
80/HTTP
443/HTTP
62.189.202.55
Linux
UUNET (702)
England, United Kingdom
network.device
443/HTTP
54.195.58.94 (ec2-54-195-58-94.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
443/HTTP
18.200.55.219 (ec2-18-200-55-219.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
80/HTTP
443/HTTP
62.189.28.163
Linux
UUNET (702)
England, United Kingdom
network.device
443/HTTP
91.185.171.46
Linux
SASEUROPE (15533)
England, United Kingdom
network.device
443/HTTP
104.18.204.64

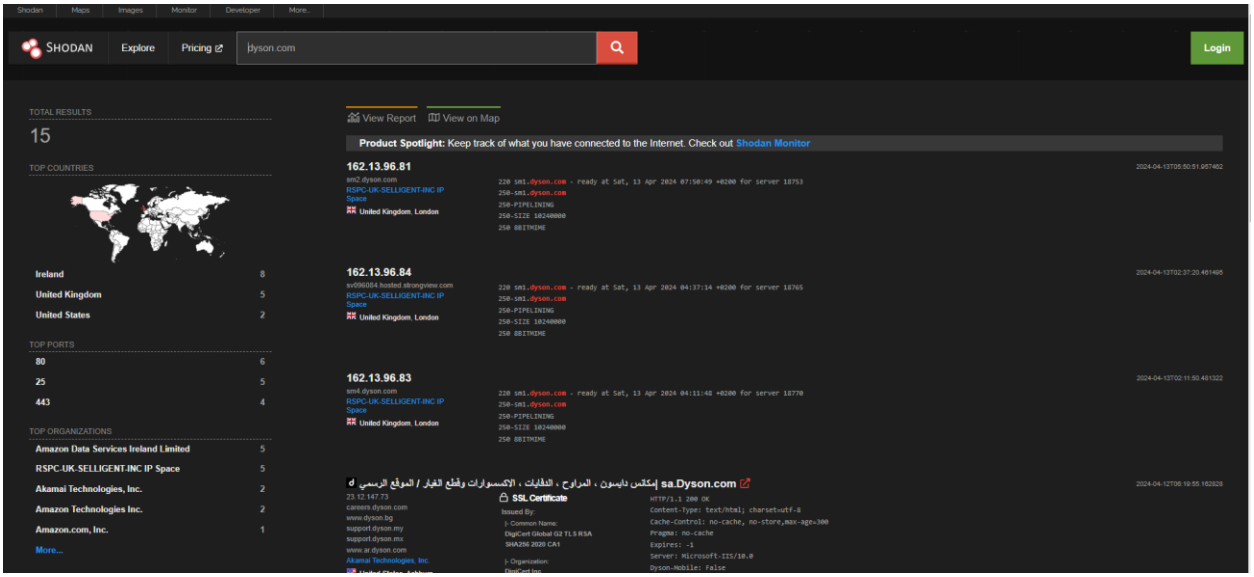

censys
Hosts
dyson.com
Search
Register
Log In
4 SNMP
More
Ports:
1,110 443
936 80
37 22
30 8443
28 8080
More
Software Vendor:
1,530 Akamai
882 Amazon
354 CloudFlare
70 nginx
43 Microsoft
More
Software Product:
765 GHost
693 CloudFront Load Balancer
354 CloudFlare Load Balancer
144 Elastic Load Balancing
113 linux
More
104.18.204.64
CLOUDFLARENET (13335)
California, United States
80/HTTP
443/HTTP
2052/HTTP
2053/HTTP
2082/HTTP
2083/HTTP
2086/HTTP
2087/HTTP
2095/HTTP
2096/HTTP
8080/HTTP
8443/HTTP
8880/HTTP
172.65.226.133
CLOUDFLARENET (13335)
California, United States
443/UNKNOWN
104.18.205.64
CLOUDFLARENET (13335)
California, United States
80/HTTP
443/HTTP
2052/HTTP
2053/HTTP
2082/HTTP
2083/HTTP
2086/HTTP
2087/HTTP
2095/HTTP
2096/HTTP
8080/HTTP
8443/HTTP
8880/HTTP
52.18.236.164 (ec2-52-18-236-164.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
default-landing-page
80/HTTP
443/HTTP
34.253.243.64 (ec2-34-253-243-64.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
80/HTTP
443/HTTP
54.72.125.63 (ec2-54-72-125-63.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
80/HTTP
443/HTTP
52.211.244.129
AMAZON-02 (16509)
Leinster, Ireland
default-landing-page
443/HTTP

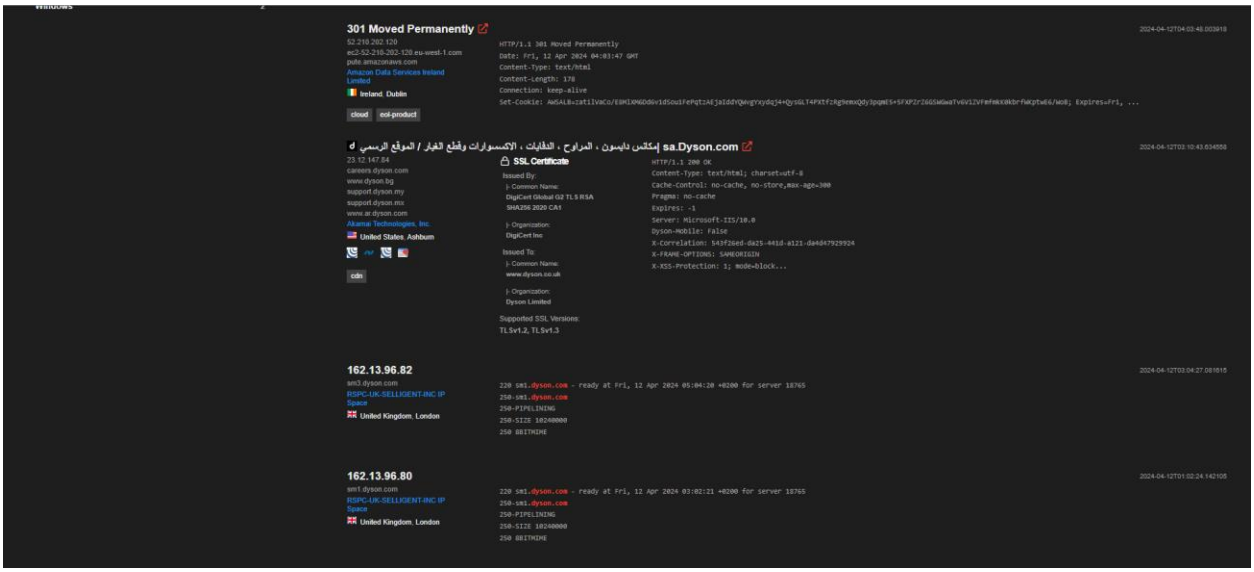

censys
Hosts
dyson.com
Search
Register
Log In
54.75.226.220 (ec2-54-75-226-220.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
80/HTTP
443/HTTP
34.242.38.74 (ec2-34-242-38-74.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
default-landing-page
80/HTTP
443/HTTP
52.213.78.140 (ec2-52-213-78-140.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
443/HTTP
62.189.202.16
Microsoft Windows
UUNET (702)
England, United Kingdom
443/HTTP
34.252.93.222 (ec2-34-252-93-222.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
443/HTTP
54.72.104.216 (ec2-54-72-104-216.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
default-landing-page
80/HTTP
443/HTTP
52.31.56.201 (ec2-52-31-56-201.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
443/HTTP
34.248.109.211 (ec2-34-248-109-211.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
default-landing-page
80/HTTP
443/HTTP

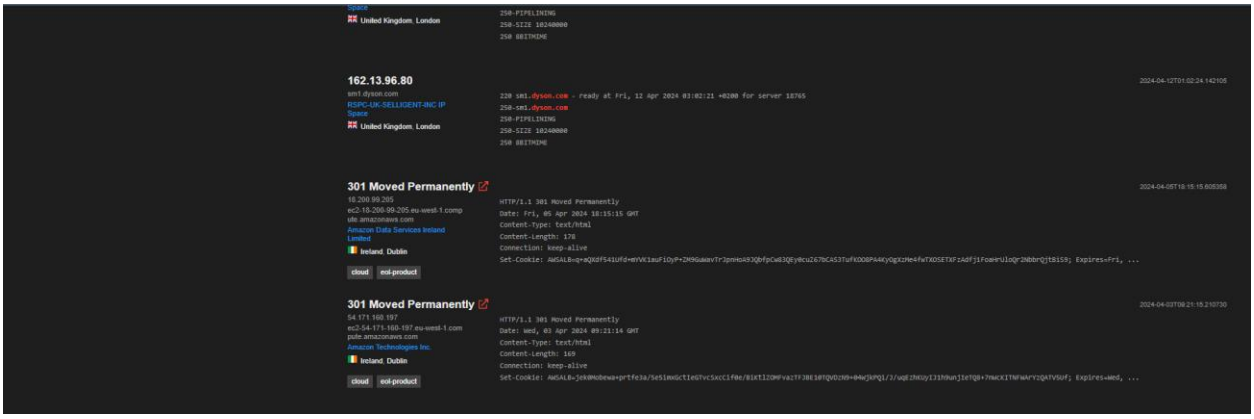

censys
Hosts
dyson.com
Search
Register
Log In
AMAZON-02 (16509)
Leinster, Ireland
443/HTTP
34.248.109.211 (ec2-34-248-109-211.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509)
Leinster, Ireland
default-landing-page
80/HTTP
443/HTTP
51.11.4.97
Microsoft
MICROSOFT-CORP-MSN-AS-BLOCK (8075)
England, United Kingdom
443/HTTP
10124/HTTP
23.210.136.142 (a23-210-136-142.deploy.static.akamaitechnologies.com)
Akamai
AKAMAI-AS (16625)
Illinois, United States
80/HTTP
443/HTTP
104.73.25.43 (a104-73-25-43.deploy.static.akamaitechnologies.com)
Akamai
AKAMAI-AS (16625)
Pennsylvania, United States
80/HTTP
443/HTTP
162.13.96.80 (sm1.dyson.com)
RACKSPACE-LON (15395)
England, United Kingdom
email
25/SMTP
80/HTTP
443/HTTP
PREVIOUS
NEXT
Pagination limited to 1.
Register or Log In
Resource Hub • Attack Surface Management • Federal • Research Access
Need Help? Help Center or support@censys.io | © 2024 Censys

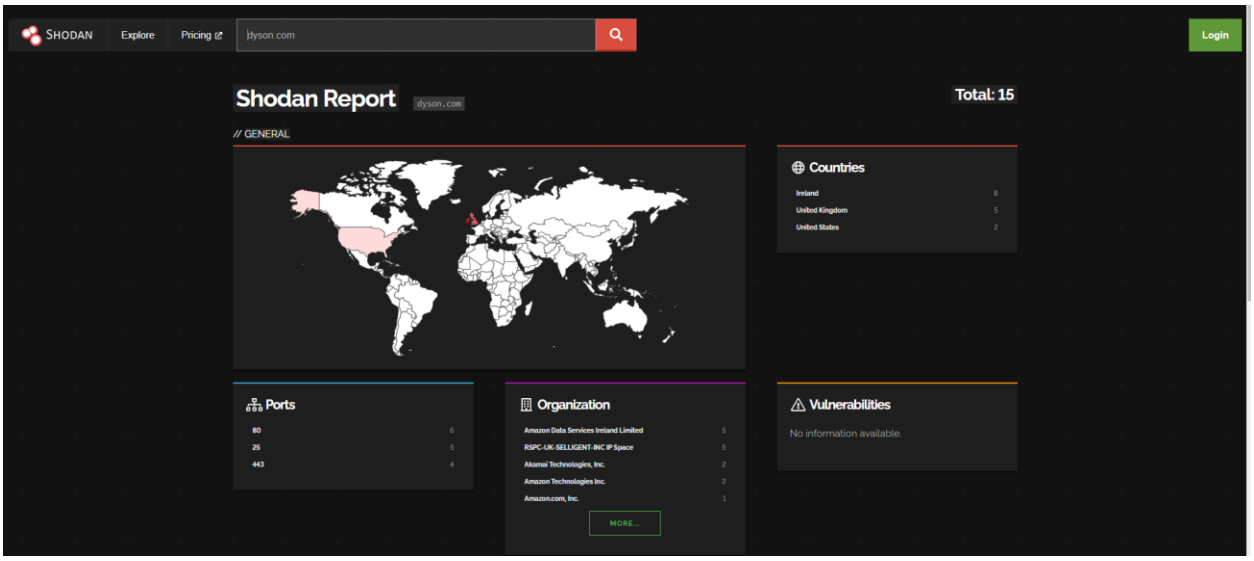
Shodan

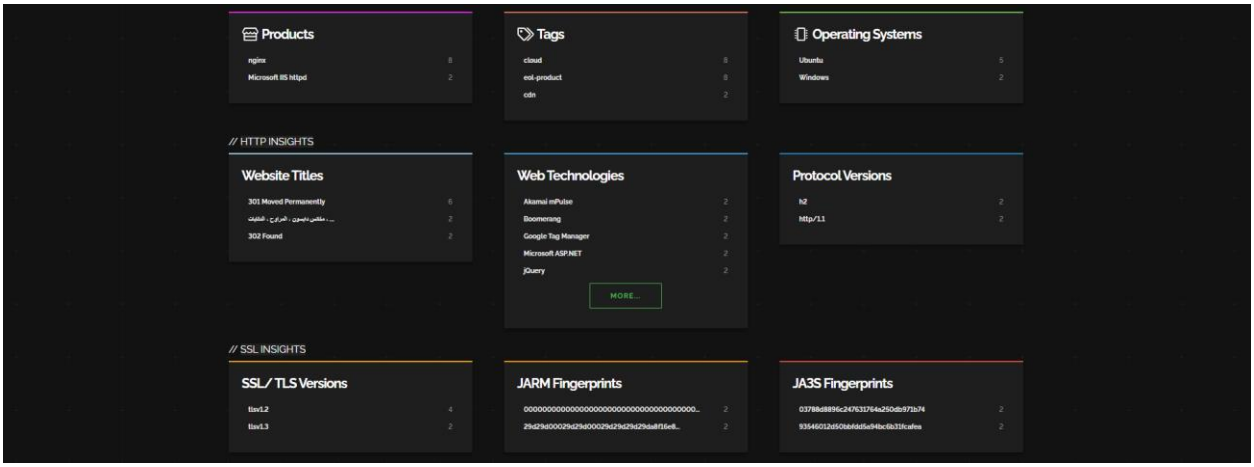
Shodan is a powerful tool for discovering and analyzing internet connected devices and services. However it is important to use Shodan responsibly and ethically respecting the privacy and security of internet users and organizations. Unauthorized scanning or exploitation of devices discovered through Shodan is illegal and unethical.






United Kingdom, London
250-PIPELINING
250-SIZE 10240000
250 8BITMIME
162.13.96.80
sm1.dyson.com
RSPC-UK-SELLIGENT-INC IP Space
United Kingdom, London
220 sm1.dyson.com - ready at Fri, 12 Apr 2024 03:02:21 +0200 for server 18765
250-sm1.dyson.com
250-PIPELINING
250-SIZE 10240000
250 8BITMIME
2024-04-12T01:02:24.142105
301 Moved Permanently
18.200.99.205
ec2-18-200-99-205.eu-west-1.compute.amazonaws.com
Amazon Data Services Ireland Limited
Ireland, Dublin
cloud
eol-product
HTTP/1.1 301 Moved Permanently
Date: Fri, 05 Apr 2024 18:15:15 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
2024-04-05T18:15:15.605358
301 Moved Permanently
54.171.160.197
ec2-54-171-160-197.eu-west-1.compute.amazonaws.com
Amazon Technologies Inc.
Ireland, Dublin
cloud
eol-product
HTTP/1.1 301 Moved Permanently
Date: Wed, 03 Apr 2024 09:21:14 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
2024-04-03T08:21:15.210730


SHODAN
Explore
Pricing
dyson.com
Login
Shodan Report
dyson.com
Total: 15
// GENERAL
Countries
Ireland 8
United Kingdom 5
United States 2
Ports
80 6
25 5
443 4
Organization
Amazon Data Services Ireland Limited 5
RSPC-UK-SELLIGENT-INC IP Space 5
Akamai Technologies, Inc. 2
Amazon Technologies Inc. 2
Amazon.com, Inc. 1
MORE...
Vulnerabilities
No information available.



File system structure

Dirb Tool

Dirb is a web content scanner and directory brute-forcing tool used for discovering hidden directories and files on web servers. It is often employed by penetration testers and security professionals to identify potential vulnerabilities in web applications and servers

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ dirb https://www.dyson.com/

_____________
DIRB v2.22
By The Dark Raver
_____________

START_TIME: Sun Apr 14 00:12:23 2024
URL_BASE: https://www.dyson.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________

GENERATED WORDS: 4612

---- Scanning URL: https://www.dyson.com/ ----
+ https://www.dyson.com/.bash_history (CODE:200|SIZE:319055)
+ https://www.dyson.com/.bashrc (CODE:200|SIZE:319055)
+ https://www.dyson.com/.cache (CODE:200|SIZE:319055)
+ https://www.dyson.com/.config (CODE:200|SIZE:319056)
+ https://www.dyson.com/.cvs (CODE:200|SIZE:319055)
+ https://www.dyson.com/.cvsignore (CODE:200|SIZE:319055)
+ https://www.dyson.com/.forward (CODE:200|SIZE:319056)
+ https://www.dyson.com/.history (CODE:200|SIZE:319055)
+ https://www.dyson.com/.listing (CODE:200|SIZE:319055)
+ https://www.dyson.com/.listings (CODE:200|SIZE:319056)
+ https://www.dyson.com/.mysql_history (CODE:200|SIZE:319055)
+ https://www.dyson.com/.passwd (CODE:200|SIZE:319055)
+ https://www.dyson.com/.perf (CODE:200|SIZE:319055)
+ https://www.dyson.com/.profile (CODE:200|SIZE:319055)
+ https://www.dyson.com/.rhosts (CODE:200|SIZE:319056)
+ https://www.dyson.com/.sh_history (CODE:200|SIZE:319055)
+ https://www.dyson.com/.ssh (CODE:200|SIZE:319055)
+ https://www.dyson.com/.subversion (CODE:200|SIZE:319055)
+ https://www.dyson.com/.svn (CODE:200|SIZE:319056)
+ https://www.dyson.com/.web (CODE:200|SIZE:319055)
+ https://www.dyson.com/_ajax (CODE:200|SIZE:319055)
+ https://www.dyson.com/_vti_bin/shtml.dll (CODE:301|SIZE:0)
+ https://www.dyson.com/about (CODE:301|SIZE:0)
+ https://www.dyson.com/About (CODE:301|SIZE:0)
+ https://www.dyson.com/admin (CODE:301|SIZE:0)
+ https://www.dyson.com/Admin (CODE:301|SIZE:0)
+ https://www.dyson.com/ADMIN (CODE:301|SIZE:0)
+ https://www.dyson.com/adserver (CODE:200|SIZE:163221)
+ https://www.dyson.com/advisories (CODE:200|SIZE:163221)
```

```
+ https://www.dyson.com/campaign (CODE:301|SIZE:0)
+ https://www.dyson.com/campaigns (CODE:200|SIZE:168669)
+ https://www.dyson.com/careers (CODE:301|SIZE:0)
+ https://www.dyson.com/cgi-bin/ (CODE:301|SIZE:236)
+ https://www.dyson.com/chat (CODE:301|SIZE:0)
+ https://www.dyson.com/check (CODE:200|SIZE:163221)
+ https://www.dyson.com/checkout (CODE:302|SIZE:0)
+ https://www.dyson.com/commercial (CODE:301|SIZE:3535)
+ https://www.dyson.com/constant (CODE:200|SIZE:163221)
+ https://www.dyson.com/contact (CODE:301|SIZE:0)
+ https://www.dyson.com/Contact (CODE:301|SIZE:0)
+ https://www.dyson.com/dbm (CODE:200|SIZE:163221)
+ https://www.dyson.com/de (CODE:301|SIZE:0)
+ https://www.dyson.com/deals (CODE:200|SIZE:1161252)
+ https://www.dyson.com/default (CODE:301|SIZE:0)
+ https://www.dyson.com/Default (CODE:301|SIZE:0)
+ https://www.dyson.com/design (CODE:301|SIZE:42184)
+ https://www.dyson.com/docs (CODE:301|SIZE:0)
+ https://www.dyson.com/download (CODE:302|SIZE:0)
+ https://www.dyson.com/downloads (CODE:200|SIZE:163221)
+ https://www.dyson.com/education (CODE:301|SIZE:28832)
+ https://www.dyson.com/em (CODE:301|SIZE:0)
+ https://www.dyson.com/en (CODE:200|SIZE:317801)
+ https://www.dyson.com/environment (CODE:301|SIZE:0)
+ https://www.dyson.com/error (CODE:200|SIZE:172244)
+ https://www.dyson.com/events (CODE:301|SIZE:0)
+ https://www.dyson.com/Events (CODE:301|SIZE:0)
+ https://www.dyson.com/facebook (CODE:200|SIZE:382239)
+ https://www.dyson.com/fb (CODE:200|SIZE:382239)
+ https://www.dyson.com/filter (CODE:200|SIZE:323303)
+ https://www.dyson.com/forms (CODE:200|SIZE:166724)
+ https://www.dyson.com/fr (CODE:301|SIZE:0)
+ https://www.dyson.com/gifts (CODE:200|SIZE:881051)
+ https://www.dyson.com/help (CODE:301|SIZE:0)
+ https://www.dyson.com/Help (CODE:301|SIZE:0)
+ https://www.dyson.com/home (CODE:301|SIZE:0)
+ https://www.dyson.com/Home (CODE:301|SIZE:0)
+ https://www.dyson.com/hotels (CODE:301|SIZE:27332)
+ https://www.dyson.com/html (CODE:301|SIZE:0)
+ https://www.dyson.com/HTML (CODE:301|SIZE:0)
+ https://www.dyson.com/index.html (CODE:301|SIZE:0)
+ https://www.dyson.com/inetpub (CODE:200|SIZE:163221)
+ https://www.dyson.com/it (CODE:301|SIZE:0)
+ https://www.dyson.com/jhtml (CODE:301|SIZE:0)
+ https://www.dyson.com/kr (CODE:301|SIZE:0)
+ https://www.dyson.com/la (CODE:302|SIZE:0)
+ https://www.dyson.com/login (CODE:301|SIZE:0)
+ https://www.dyson.com/Login (CODE:301|SIZE:0)
+ https://www.dyson.com/manual (CODE:301|SIZE:0)
+ https://www.dyson.com/monitoring (CODE:301|SIZE:0)
+ https://www.dyson.com/my (CODE:301|SIZE:0)
+ https://www.dyson.com/newsroom (CODE:200|SIZE:844614)
+ https://www.dyson.com/offices (CODE:301|SIZE:28748)
+ https://www.dyson.com/order (CODE:301|SIZE:0)
+ https://www.dyson.com/owners (CODE:301|SIZE:0)
```

Dirsearch

Dirsearch is another web content scanner and directory brute-forcing tool similar to Dirb. It's used for discovering hidden directories and fiels on web servers and it is commonly employed by security professionals and penetration testing.

```
git clone https://github.com/maurosoria/dirsearch.git
```

```
┌──(rasan㉿kali)-[~/Desktop]
└─$ git clone https://github.com/maurosoria/dirsearch.git
Cloning into 'dirsearch'...
remote: Enumerating objects: 11954, done.
remote: Counting objects: 100% (374/374), done.
remote: Compressing objects: 100% (200/200), done.
remote: Total 11954 (delta 217), reused 299 (delta 172), pack-reused 11580
Receiving objects: 100% (11954/11954), 21.62 MiB | 1.75 MiB/s, done.
Resolving deltas: 100% (7843/7843), done.
```

```
┌──(rasan㉿kali)-[~/Desktop/dirsearch]
└─$ python3 dirsearch.py -u dyson.com
Missing required dependencies to run.
Do you want dirsearch to automatically install them? [Y/n] y
Installing required dependencies...

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11722

Output: /home/rasan/Desktop/dirsearch/reports/_dyson.com/_24-04-14_03-18-24.txt

Target: http://dyson.com/

[03:18:25] Starting:
[03:18:28] 403 -  312B  - /%2e%2e//google.com
[03:18:28] 301 -  160B  - /%C0%AE%C0%AE%C0%AF  →  http://www.dyson.com/%C3%80%C2%AE%C3%80%C2%AE%
C3%80%C2%AF
[03:18:30] 301 -  150B  - /%ff  →  http://www.dyson.com/%C3%BF
[03:18:30] 404 -    1KB - /+CSCOE+/logon.html
[03:18:30] 404 -    1KB - /+CSCOE+/session_password.html
[03:18:30] 404 -    1KB - /+CSCOT+/oem-customization?app=AnyConnect&type=oem&platform=..&resource
-type=..&name=%2bCSCOE%2b/portal_inc.lua
[03:18:30] 404 -    1KB - /+CSCOT+/translation
[03:18:30] 404 -    1KB - /+CSCOT+/translation-table?type=mst&textdomain=/%2bCSCOE%2b/portal_inc.
lua&default-language&lang=../
[03:18:30] 403 -  312B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[03:18:30] 404 -    1KB - /+CSCOT+/oem
[03:18:30] 404 -    1KB - /.asa
[03:18:32] 404 -    1KB - /.config
[03:18:32] 404 -    1KB - /.config/psi+/profiles/default/accounts.xml
[03:18:39] 404 -    1KB - /.mdb
[03:18:39] 404 -    1KB - /.nuget/packages.config
[03:18:46] 403 -  312B  - /\..\..\..\..\..\..\..\..\etc\passwd
[03:18:50] 301 -  151B  - /a%5c.aspx  →  http://www.dyson.com/a/.aspx
[03:18:55] 404 -    1KB - /admin.mdb
[03:18:55] 404 -    1KB - /admin/.config
[03:19:11] 404 -    1KB - /app.config
[03:19:11] 404 -    1KB - /app/bin
[03:19:11] 404 -    1KB - /app_code
[03:19:11] 404 -    1KB - /App_Code
[03:19:11] 404 -    1KB - /App_Data
[03:19:11] 404 -    1KB - /app_data
[03:19:13] 404 -    1KB - /authorization.config
[03:19:13] 301 -  162B  - /axis//happyaxis.jsp  →  http://www.dyson.com/axis/happyaxis.jsp
[03:19:14] 301 -  173B  - /axis2//axis2-web/HappyAxis.jsp  →  http://www.dyson.com/axis2/axis2-w
eb/HappyAxis.jsp
[03:19:14] 301 -  167B  - /axis2-web//HappyAxis.jsp  →  http://www.dyson.com/axis2-web/HappyAxis
.jsp
[03:19:16] 404 -    1KB - /bin
[03:19:16] 404 -    1KB - /bin/config.sh
[03:19:16] 404 -    1KB - /bin/
[03:19:16] 404 -    1KB - /bin/reset-db.sh
```

Firewall protection against target domains

Firewall protection against target domains typically involves configuring firewall rules to restrict or control access to specific domains or IP addresses. This can be done using various techniques and features offered by firewall.

Wafw00f

Wafw00f is a Python tool designed to identify and fingerprint web application firewalls(WAFs) and other security protection mechanisms in use on a web server. It helps security professionals and penetration testers understand the security posture of web applications by detecting if they are protected by a WAF.

```
┌──(rasan㉿kali)-[~]
└─$ wafw00f

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

Usage: wafw00f url1 [url2 [url3 ... ]]
example: wafw00f http://www.victim.org/

wafw00f: error: No test target specified.
```

First I checked the main domain.

```
┌──(rasan㉿kali)-[~]
└─$ wafw00f http://dyson.com

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://dyson.com
ERROR:wafw00f:Something went wrong HTTPConnectionPool(host='www.dyson.com', port=80): Read timed out. (read t
imeout=7)
ERROR:wafw00f:Site dyson.com appears to be down
```

Using Domain name, we can't check the Firewall protection therefore now we try to use IP address of that domain.

```
┌──(rasan㉿kali)-[~]
└─$ nslookup www.dyson.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.dyson.com   canonical name = dyson.com.edgekey.net.
dyson.com.edgekey.net   canonical name = e38325.a.akamaiedge.net.
Name:   e38325.a.akamaiedge.net
Address: 23.32.29.11
Name:   e38325.a.akamaiedge.net
Address: 96.17.180.45
```

There are two IP addresses. Now we will try to check them.

```
┌──(rasan㉿kali)-[~]
└─$ wafw00f http://23.32.29.11

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://23.32.29.11
[+] The site http://23.32.29.11 is behind Kona SiteDefender (Akamai) WAF.
[~] Number of requests: 2

┌──(rasan㉿kali)-[~]
└─$ wafw00f http://96.17.180.45

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://96.17.180.45
[+] The site http://96.17.180.45 is behind Kona SiteDefender (Akamai) WAF.
[~] Number of requests: 2
```

In main domain there have Firewall protection.

Find open ports and running devices

To find open ports and running devices on a network we can use various network scanning tools with Nmap one of the most commonly used.

Nmap

Nmap short for Network mapper is a versatile open-source tool used for network discovery and security. It is one of the most popular and powerful network scanning tool available widely used by network administrators, security professionals and ethical hackers.

```
┌──(rasan㉿kali)-[~]
└─$ nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
```

```
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdd3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Nmap target domain

```
┌──(rasan㉿kali)-[~]
└─$ nmap dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-15 11:07 EDT
Nmap scan report for dyson.com (52.59.122.122)
Host is up (0.17s latency).
Other addresses for dyson.com (not scanned): 52.59.125.242
rDNS record for 52.59.122.122: ec2-52-59-122-122.eu-central-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.91 seconds
```

Top ports

```
┌──(rasan㉿kali)-[~]
└─$ nmap -top-ports 10 dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-15 11:09 EDT
Nmap scan report for dyson.com (52.59.122.122)
Host is up (0.16s latency).
Other addresses for dyson.com (not scanned): 52.59.125.242
rDNS record for 52.59.122.122: 122.122.59.52.in-addr.arpa

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   open     smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
```

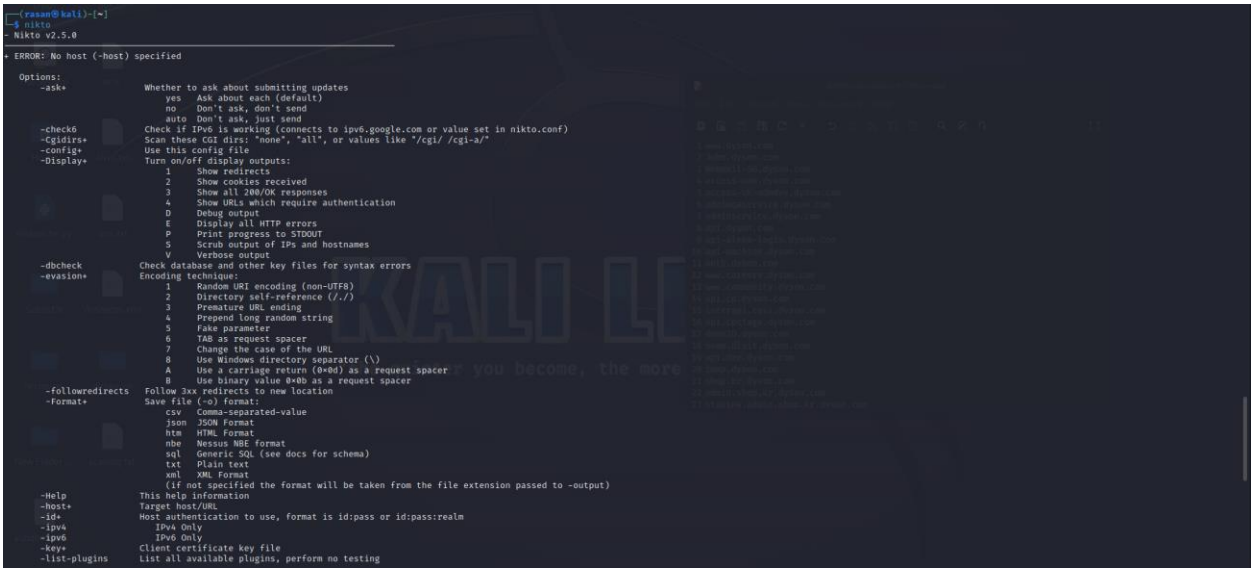
To get more information about vulnerabilities I used some tool for further scans.

Vulnerability Analyzing Phrase

Vulnerability analysis is a critical aspect of cyber security involving the identification and assessment of potential weaknesses or vulnerabilities in software systems or web applications. Nikto, wapiti,WhatWeb and Netsparker are all powerful tools commonly used in vulnerability analysis to scan web applications for security issues and provide recommendations for remediation.

Nikto

Nikto is open-source web server scanner that performs comprehensive tests against web servers for known vulnerabilities, misconfigurations and security loopholes. It scans for over 6700 potentially dangerous files, checks for outdated versions of over 1250 servers and identifies various server specific issues. Nikto also checks for potentially sensitive files and directories, outdated software versions and common security misconfigurations.



```
┌──(rasan㉿kali)-[~]
└─$ nikto
- Nikto v2.5.0
---------------------------------------------------------------------------
+ ERROR: No host (-host) specified

   Options:
       -ask+               Whether to ask about submitting updates
                               yes   Ask about each (default)
                               no    Don't ask, don't send
                               auto  Don't ask, just send
       -check6             Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                               1     Show redirects
                               2     Show cookies received
                               3     Show all 200/OK responses
                               4     Show URLs which require authentication
                               D     Debug output
                               E     Display all HTTP errors
                               P     Print progress to STDOUT
                               S     Scrub output of IPs and hostnames
                               V     Verbose output
       -dbcheck            Check database and other key files for syntax errors
       -evasion+           Encoding technique:
                               1     Random URI encoding (non-UTF8)
                               2     Directory self-reference (/./)
                               3     Premature URL ending
                               4     Prepend long random string
                               5     Fake parameter
                               6     TAB as request spacer
                               7     Change the case of the URL
                               8     Use Windows directory separator (\)
                               A     Use a carriage return (0x0d) as a request spacer
                               B     Use binary value 0x0b as a request spacer
       -followredirects    Follow 3xx redirects to new location
       -Format+            Save file (-o) format:
                               csv   Comma-separated-value
                               json  JSON Format
                               htm   HTML Format
                               nbe   Nessus NBE format
                               sql   Generic SQL (see docs for schema)
                               txt   Plain text
                               xml   XML Format
                               (if not specified the format will be taken from the file extension passed to -output)
       -Help               This help information
       -host+              Target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -ipv4                 IPv4 Only
       -ipv6                 IPv6 Only
       -key+               Client certificate key file
       -list-plugins       List all available plugins, perform no testing
```

```
-ipv4                IPv4 Only
-ipv6                IPv6 Only
-key+            Client certificate key file
-list-plugins    List all available plugins, perform no testing
-maxtime+        Maximum testing time per host (e.g., 1h, 60m, 3600s)
-mutate+         Guess additional file names:
-mutate-options  Provide information for mutates
-nointeractive   Disables interactive features
-nolookup        Disables DNS lookups
-nossl           Disables the use of SSL
-noslash         Strip trailing slash from URL (e.g., '/admin/' to '/admin')
-no404           Disables nikto attempting to guess a 404 page
-Option          Over-ride an option in nikto.conf, can be issued multiple times
-output+         Write output to this file ('.' for auto-name)
-Pause+          Pause between tests (seconds)
-Plugins+        List of plugins to run (default: ALL)
-port+           Port to use (default 80)
-RSAcert+        Client certificate file
-root+           Prepend root value to all requests, format is /directory
-Save            Save positive responses to this directory ('.' for auto-name)
-ssl             Force ssl mode on port
-Tuning+         Scan tuning:
                      1     Interesting File / Seen in logs
                      2     Misconfiguration / Default File
                      3     Information Disclosure
                      4     Injection (XSS/Script/HTML)
                      5     Remote File Retrieval - Inside Web Root
                      6     Denial of Service
                      7     Remote File Retrieval - Server Wide
                      8     Command Execution / Remote Shell
                      9     SQL Injection
                      0     File Upload
                      a     Authentication Bypass
                      b     Software Identification
                      c     Remote Source Inclusion
                      d     WebService
                      e     Administrative Console
                      x     Reverse Tuning Options (i.e., include all except specified)
-timeout+        Timeout for requests (default 10 seconds)
-Userdbs         Load only user databases, not the standard databases
                      all   Disable standard dbs and load only user dbs
                      tests Disable only db_tests and load udb_tests
-useragent       Over-rides the default useragent
-until           Run until the specified time or duration
-url+            Target host/URL (alias of -host)
-usecookies      Use cookies from responses in future requests
-useproxy        Use the proxy defined in nikto.conf, or argument http://server:port
-Version         Print plugin and database versions
-vhost+          Virtual host (for Host header)
-404code         Ignore these HTTP codes as negative responses (always). Format is "302,301".
-404string       Ignore this string in response body content as negative response (always). Can be a regular expression

                 + requires a value
```

Wapiti

Wapiti is open source web application vulnerability scanner that helps identify security vulnerabilities in web applications. It is designed to perform black box testing by sending various HTTP requests and analyzing the responses to detect potential vulnerabilities.

- Vulnerability Detection - Wapiti can detect various types of vulnerabilities, including SQL injection, cross-site scripting (XSS), command injection, file inclusion and more. It analyzes the HTTP responses from the target web application to identify potential security flaws.

- Customizable - Wapiti offers a high degree of customization allowing users to define custom injection payloads, specify scanning parameters and configure various options according to their specific requirements.

- Multi-threaded Scanning - Wapiti utilizes multi threading to improve scanning efficiency allowing it to perform simultaneous requests and speed up the scanning process.

- Reporting - After completing the scan Wapiti generates detailed reports that summarize the vulnerabilities identified during the scanning process. These reports typically include information about the vulnerabilities found, their severity levels and recommendations for remediation.

- Integration- Wapiti can be integrated into automated testing processes or used as a standalone tool for manual security assessments. It supports various output formats making it compatible with different reporting and analysis tools.

```
┌──(rasan㉿kali)-[~]
└─$ wapiti

   __   __                  _ _ _   _ ____
   / /_ \ \__ _ _ __ (_)_(_)___ /
   \ V  V / _` | '_ \| | _ | | |_ \
    \  ^  / (_| | |_) | | |_| | |__) |
     V  V \__,_| .__/|_|\__|_|____/
               |_|
Wapiti-3.0.4 (wapiti.sourceforge.io)
usage: wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}] [-m MODULES_LIST] [--list-modules] [--update] [-l LEVEL] [-p PROXY_URL] [--tor] [-a CREDENTIALS] [--auth-type {basic,digest,kerberos,ntlm,post}] [-c COOKIE_FILE]
              [--skip-crawl] [--resume-crawl] [--flush-attacks] [--flush-session] [--store-session PATH] [--store-config PATH] [-s URL] [-x URL] [-r PARAMETER] [--skip PARAMETER] [-d DEPTH] [--max-links-per-page MAX]
              [--max-files-per-dir MAX] [--max-scan-time SECONDS] [--max-attack-time SECONDS] [--max-parameters MAX] [-S FORCE] [-t SECONDS] [-H HEADER] [-A AGENT] [--verify-ssl {0,1}] [--color] [-v LEVEL] [-f FORMAT] [-o OUPUT_PATH]
              [--external-endpoint EXTERNAL_ENDPOINT_URL] [--internal-endpoint INTERNAL_ENDPOINT_URL] [--endpoint ENDPOINT_URL] [--no-bugreport] [--version]
wapiti: error: one of the arguments -u/--url --list-modules --update is required
```

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -h

   __   __                  _ _ _   _ ____
   / /_ \ \__ _ _ __ (_)_(_)___ /
   \ V  V / _` | '_ \| | _ | | |_ \
    \  ^  / (_| | |_) | | |_| | |__) |
     V  V \__,_| .__/|_|\__|_|____/
               |_|
Wapiti-3.0.4 (wapiti.sourceforge.io)
usage: wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}] [-m MODULES_LIST] [--list-modules] [--update] [-l LEVEL] [-p PROXY_URL] [--tor] [-a CREDENTIALS] [--auth-type {basic,digest,kerberos,ntlm,post}] [-c COOKIE_FILE]
              [--skip-crawl] [--resume-crawl] [--flush-attacks] [--flush-session] [--store-session PATH] [--store-config PATH] [-s URL] [-x URL] [-r PARAMETER] [--skip PARAMETER] [-d DEPTH] [--max-links-per-page MAX]
              [--max-files-per-dir MAX] [--max-scan-time SECONDS] [--max-attack-time SECONDS] [--max-parameters MAX] [-S FORCE] [-t SECONDS] [-H HEADER] [-A AGENT] [--verify-ssl {0,1}] [--color] [-v LEVEL] [-f FORMAT] [-o OUPUT_PATH]
              [--external-endpoint EXTERNAL_ENDPOINT_URL] [--internal-endpoint INTERNAL_ENDPOINT_URL] [--endpoint ENDPOINT_URL] [--no-bugreport] [--version]

Wapiti-3.0.4: Web application vulnerability scanner

options:
  -h, --help            show this help message and exit
  -u URL, --url URL     The base URL used to define the scan scope (default scope is folder)
  --scope {page,folder,domain,url,punk}
                        Set scan scope
  -m MODULES_LIST, --module MODULES_LIST
                        List of modules to load
  --list-modules        List Wapiti attack modules and exit
  --update              Update Wapiti attack modules and exit
  -l LEVEL, --level LEVEL
                        Set attack level
  -p PROXY_URL, --proxy PROXY_URL
                        Set the HTTP(S) proxy to use. Supported: http(s) and socks proxies
  --tor                 Use Tor listener (127.0.0.1:9050)
  -a CREDENTIALS, --auth-cred CREDENTIALS
                        Set HTTP authentication credentials
  --auth-type {basic,digest,kerberos,ntlm,post}
                        Set the authentication type to use
  -c COOKIE_FILE, --cookie COOKIE_FILE
                        Set a JSON cookie file to use
  --skip-crawl          Don't resume the scanning process, attack URLs scanned during a previous session
  --resume-crawl        Resume the scanning process (if stopped) even if some attacks were previously performed
  --flush-attacks       Flush attack history and vulnerabilities for the current session
  --flush-session       Flush everything that was previously found for this target (crawled URLs, vulns, etc)
  --store-session PATH  Directory where to store attack history and session data.
  --store-config PATH   Directory where to store configuration databases.
  -s URL, --start URL   Adds an url to start scan with
  -x URL, --exclude URL
                        Adds an url to exclude from the scan
  -r PARAMETER, --remove PARAMETER
                        Remove this parameter from urls
  --skip PARAMETER      Skip attacking given parameter(s)
  -d DEPTH, --depth DEPTH
                        Set how deep the scanner should explore the website
  --max-links-per-page MAX
                        Set how many (in-scope) links the scanner should extract for each page
  --max-files-per-dir MAX
```

WhatWeb

WhatWeb is powerful web application scanner that identifies the technologies used on websites. It analyzes HTTP response headers, HTML content and other web artifacts to determine the web server, programming language, CMS (Content Management System) and other components utilized in the target application.

- Technology Detection - WhatWeb employs fingerprinting techniques to identify the technologies and frameworks utilized in web applications. It can detect web servers (such as Apache, Nginx, IIS), programming languages (PHP, ASP.NET, Python), CMS platforms (WordPress, Joomla, Drupal), JavaScript libraries (jQuery, AngularJS) and more.

- Extensive Plugin Support - WhatWeb supports wide range of plugins that extend its capabilities for detecting specific technologies and vulnerabilities associated with them. These plugins enable

WhatWeb to identify additional details about the target application is technology stack and potential security weaknesses.

- Customizable- WhatWeb allows users to customize the scanning process by specifying various options and parameters. Users can define custom plugin configurations, adjust the scanning depth and control the verbosity of the output according to their specific requirements.

- Output Formats- WhatWeb provides flexible output formats, including plain text, JSON, XML and HTML allowing users to choose the format that best suits their needs. The generated reports include detailed information about the detected technologies, their versions and other relevant details.

- Integration- WhatWeb can be integrated into automated testing frameworks or used as a standalone tool for manual security assessments. It supports command line usage making it easy to incorporate into scripts and workflows for efficient scanning and analysis.

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 52.59.125.242, 52.59.122.122
+ Target IP:          52.59.125.242
+ Target Hostname:    dyson.com
+ Target Port:        80
+ Start Time:         2024-04-16 00:33:30 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers
/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differ
ent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-hea
der/
+ Root page / redirects to: http://www.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7963 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-04-16 01:09:12 (GMT-4) (2142 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

➢ **The anti-clickjacking X-Frame-Option header is not present**

This finding indicates that the web server is not utilizing the X-Frame-Options header to mitigate clickjacking attacks. Clickjacking is a technique where an attacker tricks a user into clicking on a disguised element on a web page. By implementing X-Frame-Options with the proper settings the web server can prevent its content from being embedded into other sites via iframes thereby reducing the risk of clickjacking attacks.

➢ **The X-Content-Type-Options header is not set**

This finding indicates that the web server is not utilizing the X-Content-Type-Options header. This header is used to prevent MIME-sniffing attacks by instructing the browser to honor the declared content type and not to override it based on content inspection. Without this header, there is a risk that browsers may incorrectly interpret the content type potentially leading to security vulnerabilities.

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u http://dyson.com/
    __  __                _  __  __ _____
   / / ^ \ \__ _ _ __ (_) |_(_)___ /
   \ V  V / _` | '_ \| | __| | |_ \
    \  ^  / (_| | |_) | | |_| |___) |
     V  V \__,_| .__/|_|\__|_|____/
                |_|
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ========
This scan has been saved in the file /home/rasan/.wapiti/scans/dyson.com_folder_8a1cd1fb.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
         backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods,
nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
Problem with local wapp database.
Downloading from the web ...

[*] Launching module csp
1 requests were skipped due to network issues

[*] Launching module http_headers
1 requests were skipped due to network issues

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=tqq3sa for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
 ======
A report has been generated in the file /home/rasan/.wapiti/generated_report
Open /home/rasan/.wapiti/generated_report/dyson.com_04162024_1700.html with a browser to see this report.
```

It automatically generate the report

Wapiti vulnerability report

Target: http://dyson.com/

Date of the scan: Tue, 16 Apr 2024 17:00:12 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	0
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	0
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Wapiti 3.0.4 © Nicolas SURRIBAS 2006-2021

Zero vulnerabilities found.

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 dyson.com
WhatWeb report for http://dyson.com
Status    : 301 Moved Permanently
Title     : Document Moved
IP        : 52.59.125.242
Country   : UNITED STATES, US

Summary   : HTTPServer[Microsoft-IIS/7.5], Microsoft-IIS[7.5], RedirectLocation[http://www.dyson.com/], X-Powered-By[ASP.NET]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-IIS/7.5 (from server string)

[ Microsoft-IIS ]
        Microsoft Internet Information Services (IIS) for Windows
        Server is a flexible, secure and easy-to-manage Web server
        for hosting anything on the Web. From media streaming to
        web application hosting, IIS's scalable and open
        architecture is ready to handle the most demanding tasks.

        Version      : 7.5
        Website      : http://www.iis.net/

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : http://www.dyson.com/ (from location)

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : ASP.NET (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Content-Type: text/html; charset=UTF-8
        Location: http://www.dyson.com/
        Server: Microsoft-IIS/7.5
        X-Powered-By: ASP.NET
        Date: Tue, 16 Apr 2024 17:06:54 GMT
        Connection: close
        Content-Length: 144

WhatWeb report for http://www.dyson.com/
Status    : 403 Forbidden
Title     : Access Denied
IP        : 184.50.85.154
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost], UncommonHeaders[server-timing]
```

```
Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website      : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : AkamaiGHost (from server string)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : server-timing (from headers)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 365
        Expires: Tue, 16 Apr 2024 17:06:58 GMT
        Date: Tue, 16 Apr 2024 17:06:58 GMT
        Connection: close
        Server-Timing: cdn-cache; desc=HIT
        Server-Timing: edge; dur=1
        Server-Timing: ak_p; desc="1713287218083_3090306454_20679381_18_138487_248_0_-";dur=1
```

Does not find any vulnerabilities.

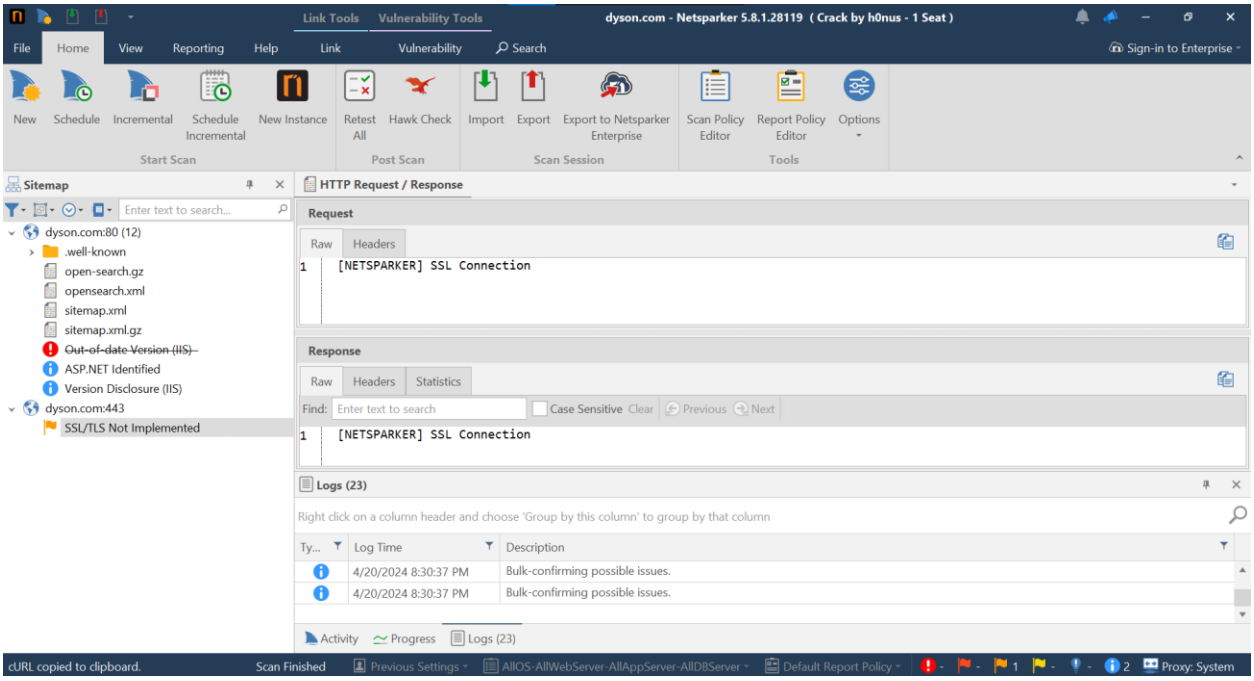
- **Nmap**

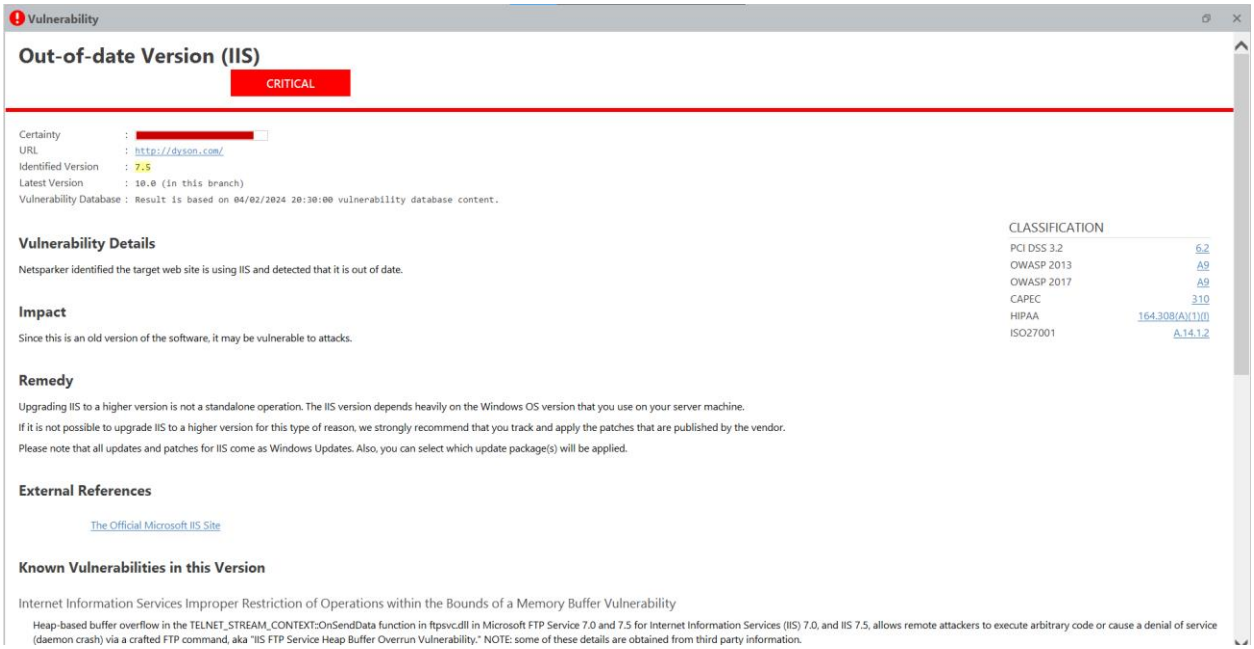
```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-16 13:02 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
PACKET TRACE: enabled
NSOCK INFO [0.000000] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.000000] nsock_connect_udp(): TCP connection requested to 192.168.1.1:53 (IOD #1) EOL
NSOCK INFO [0.000000] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.000000] nsock_connect_udp(): TCP connection requested to 192.168.1.1:53 (IOD #2) EOL
NSOCK INFO [0.000000] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [0.000000] nsock_connect_udp(): TCP connection requested to 192.168.1.1:53 (IOD #3) EOL
NSOCK INFO [0.000000] nsock_iod_new2(): nsock_iod_new (IOD
```

- **Netsparker**

With the aid of Netsparker (Invicti), an automated online application security scanner that offers a substantial degree of configurability in addition to its scanning capabilities, websites, web applications, and web services can be examined. Using this scanner, you will be able to find security flaws in your website, apps, and services. While different platforms and programming languages were utilized in the development of different types of online applications, Invicti is capable of conducting scans on each of these variations.

Recordedfuture.com is being scanned for vulnerabilities using Netsparker professional Edition (V).





Vulnerability

Out-of-date Version (IIS)

CRITICAL

Certainty :
URL : http://dyson.com/
Identified Version : 7.5
Latest Version : 10.0 (in this branch)
Vulnerability Database : Result is based on 04/02/2024 20:30:00 vulnerability database content.

Vulnerability Details

Netsparker identified the target web site is using IIS and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Upgrading IIS to a higher version is not a standalone operation. The IIS version depends heavily on the Windows OS version that you use on your server machine.

If it is not possible to upgrade IIS to a higher version for this type of reason, we strongly recommend that you track and apply the patches that are published by the vendor.

Please note that all updates and patches for IIS come as Windows Updates. Also, you can select which update package(s) will be applied.

External References

The Official Microsoft IIS Site

Known Vulnerabilities in this Version

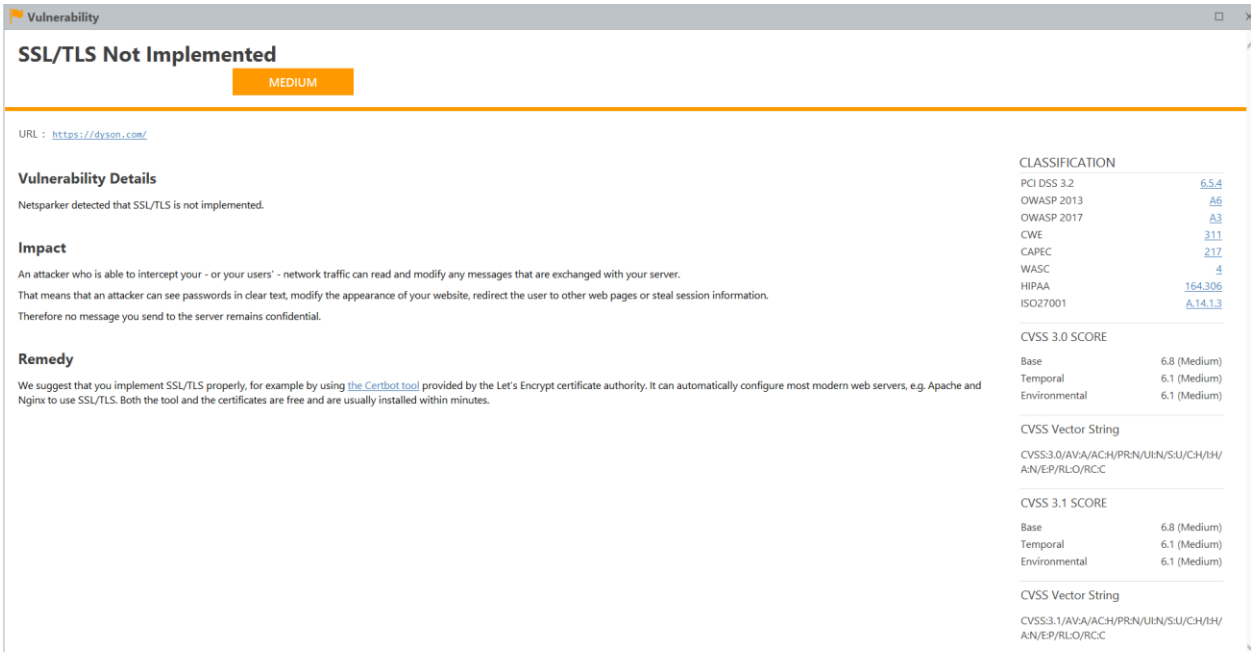
Internet Information Services Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.

CLASSIFICATION

PCI DSS 3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CAPEC	310
HIPAA	164.308(A)(1)(I)
ISO27001	A.14.1.2

Given this information it is clear that maintaining an updated version of IIS is crucial for ensuring the security of the website. Upgrading to a higher version or applying patches as recommended can help mitigate the risk of potential attacks.



Vulnerability

SSL/TLS Not Implemented

MEDIUM

URL : https://dyson.com/

Vulnerability Details

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	311
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

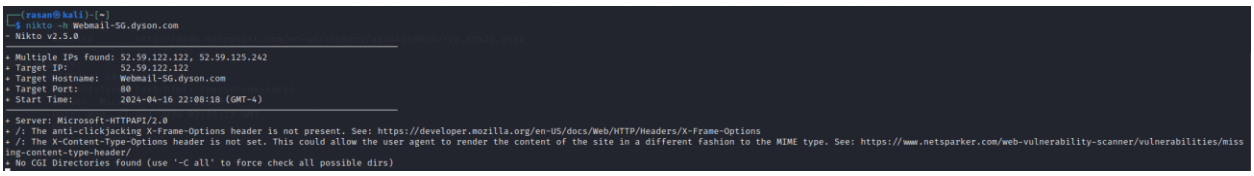
addressing this vulnerability by implementing SSL/TLS is crucial for ensuring the confidentiality and integrity of the website's communication with users and to mitigate the risks associated with potential attacks

Report 02

Target sub domain : Webmail-SG.dyson.com

<u>Vulnerability Analyzing Phrase & Recommendation</u>

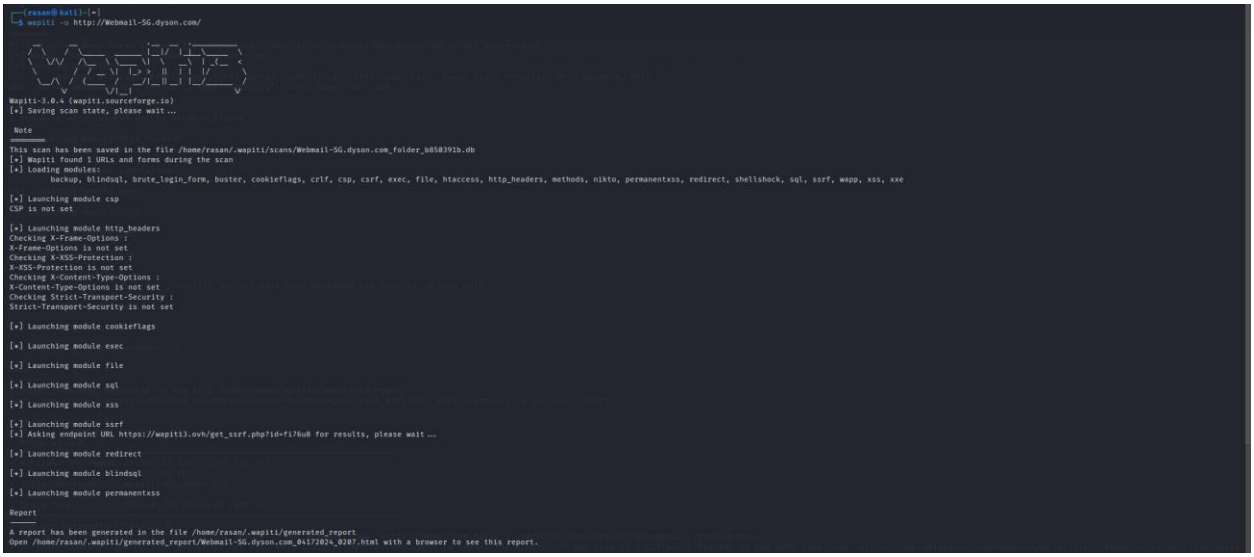
- **Nikto**



```
┌──(rasan㉿kali)-[~]
└─$ nikto -h Webmail-SG.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 52.59.122.122, 52.59.125.242
+ Target IP:          52.59.122.122
+ Target Hostname:    Webmail-SG.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-16 22:08:18 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

- ➢ The anti-clickjacking X-Frame-Options header is not present.
- ➢ The X-Content-Type-Options header is not set.

- **Wapiti**



```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u http://Webmail-SG.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[+] Saving scan state, please wait ...

 Note
 ========
This scan has been saved in the file /home/rasan/.wapiti/scans/Webmail-SG.dyson.com_folder_b850391b.db
[+] Wapiti found 1 URLs and forms during the scan
[+] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[+] Launching module csp
CSP is not set

[+] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[+] Launching module cookieflags

[+] Launching module exec

[+] Launching module file

[+] Launching module sql

[+] Launching module xss

[+] Launching module ssrf
[+] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=fi76u8 for results, please wait ...

[+] Launching module redirect

[+] Launching module blindsql

[+] Launching module permanentxss

Report
------
A report has been generated in the file /home/rasan/.wapiti/generated_report
Open /home/rasan/.wapiti/generated_report/Webmail-SG.dyson.com_04172024_0287.html with a browser to see this report.
```

Wapiti vulnerability report

Target: http://Webmail-SG.dyson.com/

Date of the scan: Wed, 17 Apr 2024 02:07:25 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0

- **Content security policy configuration**

Content Security Policy (CSP) is added layer of security that helps to detect and mitigate certain types of attacks including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability – CSP not found.

Solutions - Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowe to load for that page.

- **HTTP secure Headers**

  HTTP security headers tell the browser how to behave when handling the website is content.

  Vulnerabilities

  - X frame options is not set
  - X – XSS protection is not set
  - X-content-type options in not set
  - Strict-transport-security is not set

  Solution - Use recommendations for hardening HTTP Security Headers.

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 Webmail-SG.dyson.com
WhatWeb report for http://webmail-sg.dyson.com/
Status    : 404 Not Found
Title     : Not Found
IP        : 52.59.122.122
Country   : UNITED STATES, US

Summary   : HTTPServer[Microsoft-HTTPAPI/2.0], Microsoft-HTTPAPI[2.0]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-HTTPAPI/2.0 (from server string)

[ Microsoft-HTTPAPI ]
        The HTTP Server API enables applications to communicate
        over HTTP without using Microsoft Internet Information
        Server (IIS). Applications can register to receive HTTP
        requests for particular URLs, receive HTTP requests, and
        send HTTP responses. The HTTP Server API includes SSL
        support so that applications can exchange data over secure
        HTTP connections without IIS. It is also designed to work
        with I/O completion ports.

        Version      : 2.0
        Website      : http://msdn.microsoft.com/en-us/library/aa364510%28v=vs.85%29.aspx

HTTP Headers:
        HTTP/1.1 404 Not Found
        Content-Type: text/html; charset=us-ascii
        Server: Microsoft-HTTPAPI/2.0
        Date: Wed, 17 Apr 2024 02:35:23 GMT
        Connection: close
        Content-Length: 315
```

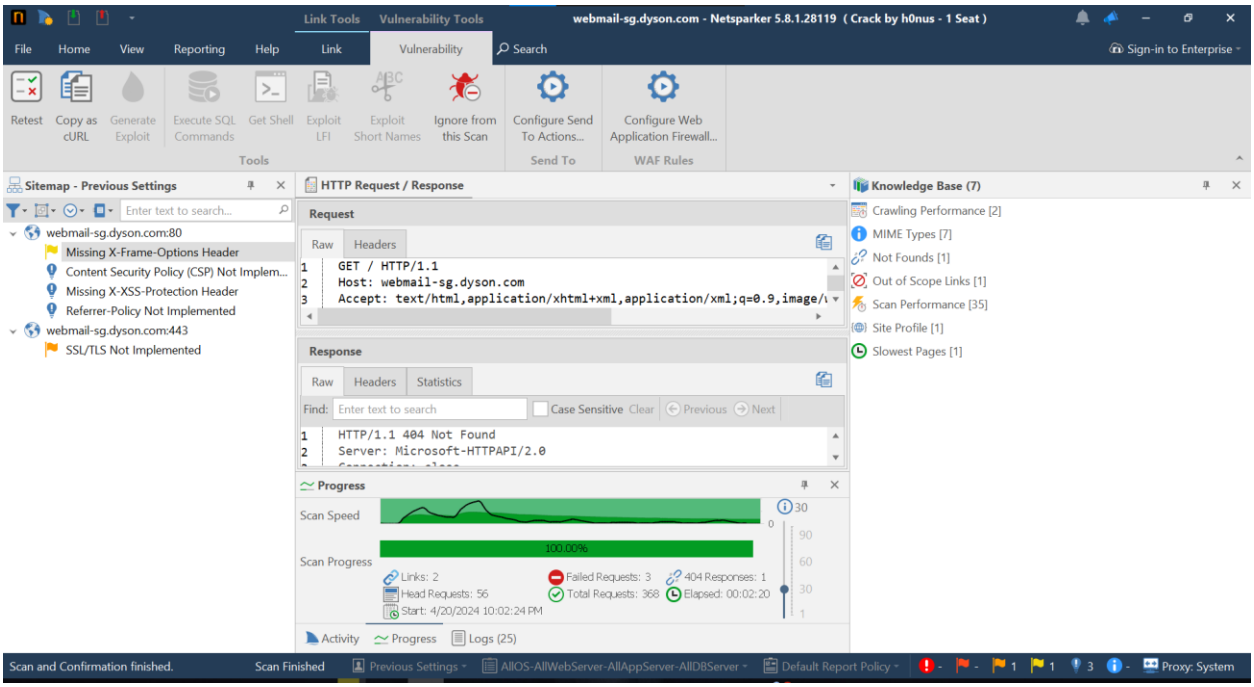
Does not find any vulnerabilities.

- **Nmap**

```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -vd --script vuln Webmail-SG.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-16 22:13 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
PLUGIN SCAN: Timing report
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
NSE: Script Pre-scanning.
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:13
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 22:13, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:13
Completed NSE at 22:13, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 22:13
mass_rdns: 0.34s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 22:13, 0.34s elapsed
DNS resolution of 1 IPs took 0.34s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 22:13
Scanning Webmail-SG.dyson.com (52.59.125.242) [1000 ports]
Discovered open port 25/tcp on 52.59.125.242
Discovered open port 80/tcp on 52.59.125.242
Discovered open port 443/tcp on 52.59.125.242
Completed Connect Scan at 22:13, 8.63s elapsed (1000 total ports)
Overall sending rates: 231.97 packets / s.
NSE: Script scanning 52.59.125.242.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:13
NSE: Starting http-vuln-misfortune-cookie against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: Starting http-phpmyadmin-dir-traversal against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: [http-phpmyadmin-dir-traversal 52.59.125.242:443] HTTP POST Webmail-SG.dyson.com/phpMyAdmin-2.6.4-pl1/libraries/grab_globals.lib.php
NSE: [http-phpmyadmin-dir-traversal 52.59.125.242:443] POST DATA usesubform[1]=1&usesubform[2]=1&subform[1][redirect]=../../../../../etc/passwd&subform[1][cXIb8O3]=1
NSE: Starting rsa-vuln-roca against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: Starting http-method-tamper against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: Starting http-vuln-cve2013-8156 against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: Starting http-stored-xss against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: Starting http-vuln-cve2017-5638 against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: Starting http-aspnet-debug against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: Starting http-frontpage-login against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: Starting http-litespeed-sourcecode-download against Webmail-SG.dyson.com (52.59.125.242:80).
NSE: [http-litespeed-sourcecode-download 52.59.125.242:80] Trying to download the source code of /index.php
NSE: Starting http-fileupload-exploiter against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: Starting http-huawei-hg5xx-vuln against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: Starting http-vuln-cve2014-3704 against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: [http-vuln-cve2014-3704 52.59.125.242:443] adding admin user (username: 'bwiwgopicy'; passwd: 'lbzytzwyuo')
NSE: Starting sslv2-drown against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: Starting http-vuln-cve2012-1823 against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: Starting http-litespeed-sourcecode-download against Webmail-SG.dyson.com (52.59.125.242:443).
NSE: [http-litespeed-sourcecode-download 52.59.125.242:443] Trying to download the source code of /index.php
NSE: Starting http-vuln-cve2014-2127 against Webmail-SG.dyson.com (52.59.125.242:443).
```

While the scan did not identify any vulnerabilities.

- **Netsparker**



Vulnerability

Missing X-Frame-Options Header

LOW

Certainty :

URL : http://webmail-sg.dyson.com/

Vulnerability Details

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

- `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
- `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
- `X-Frame-Options: ALLOW-FROM URL` It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

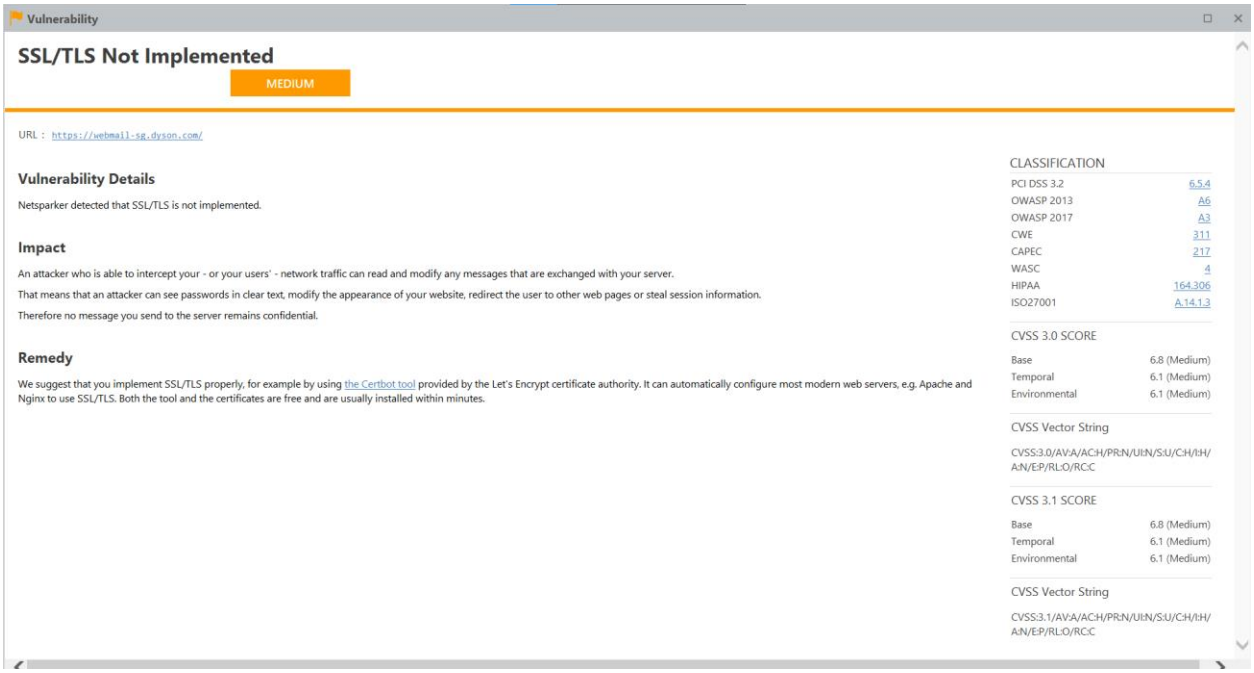
External References

Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

Remedy References

Clickjacking Defense Cheat Sheet

Addressing this vulnerability by implementing the X Frame Options header is crucial for protecting the website from clickjacking attacks and ensuring the security of user interactions.



Vulnerability

SSL/TLS Not Implemented

MEDIUM

URL : https://webmail-sg.dyson.com/

Vulnerability Details

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	311
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Addressing this vulnerability by implementing SSL/TLS is crucial for safeguarding the confidentiality and integrity of the website is communication with users and mitigating the risks associated with potential attacks.

Report 03

Target sub domain : adminqaservice.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h adminqaservice.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 52.59.122.122, 52.59.125.242, 64:ff9b::343b:7a7a, 64:ff9b::343b:7df2
+ Target IP:          52.59.122.122
+ Target Hostname:    adminqaservice.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-16 22:46:49 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+C all
- STATUS: Completed 6430 requests (~92% complete, 4.5 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.40013 sec, 10 requests: 0.4094 sec.
+ 8060 requests: 1 error(s) and 2 item(s) reported on remote host
+ End Time:           2024-04-16 23:55:14 (GMT-4) (4105 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- ➢ The anti-clickjacking X-Frame-Options header is not present
- ➢ The X-Content-Type-Options header is not set

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u http://adminqaservice.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Resuming scan from previous session, please wait
[*] Saving scan state, please wait...

 Note
This scan has been saved in the file /home/rasan/.wapiti/scans/adminqaservice.dyson.com_folder_78b24aed.db
[*] Wapiti found 3 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=h2eckj for results, please wait...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
A report has been generated in the file /home/rasan/.wapiti/generated_report
```

Wapiti vulnerability report

Target: http://adminqaservice.dyson.com/

Date of the scan: Wed, 17 Apr 2024 02:50:27 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	2
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	8
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0

- CSP is not set
- X-Frame-Options is not set
- X-XSS-Protection is not set
- X-Content-Type-Options is not set
- Strict-Transport-Security is not set
- X-Frame-Options is not set
- X-XSS-Protection is not set
- X-Content-Type-Options is not set
- Strict-Transport-Security is not set

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 adminqaservice.dyson.com
WhatWeb report for http://adminqaservice.dyson.com
Status    : 404 Not Found
Title     : Not Found
IP        : 52.59.125.242
Country   : UNITED STATES, US

Summary   : HTTPServer[Microsoft-HTTPAPI/2.0], Microsoft-HTTPAPI[2.0]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-HTTPAPI/2.0 (from server string)

[ Microsoft-HTTPAPI ]
        The HTTP Server API enables applications to communicate
        over HTTP without using Microsoft Internet Information
        Server (IIS). Applications can register to receive HTTP
        requests for particular URLs, receive HTTP requests, and
        send HTTP responses. The HTTP Server API includes SSL
        support so that applications can exchange data over secure
        HTTP connections without IIS. It is also designed to work
        with I/O completion ports.

        Version      : 2.0
        Website     : http://msdn.microsoft.com/en-us/library/aa364510%28v=vs.85%29.aspx

HTTP Headers:
        HTTP/1.1 404 Not Found
        Content-Type: text/html; charset=us-ascii
        Server: Microsoft-HTTPAPI/2.0
        Date: Wed, 17 Apr 2024 03:44:16 GMT
        Connection: close
        Content-Length: 315
```

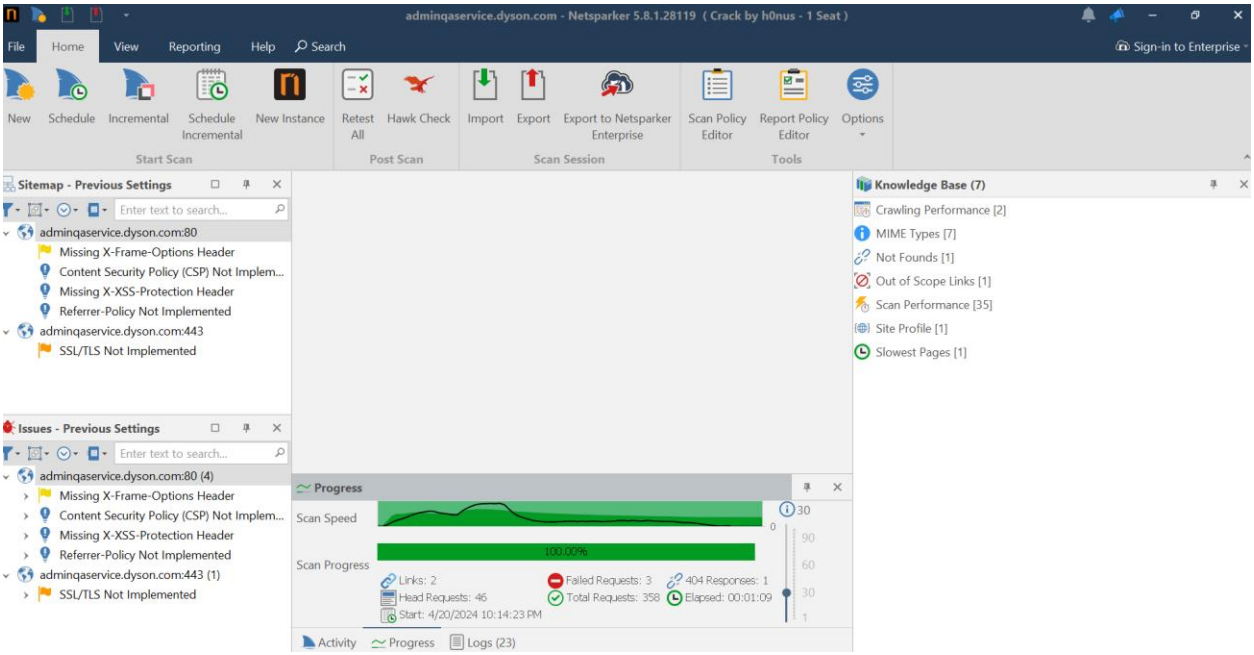
- **Nmap**

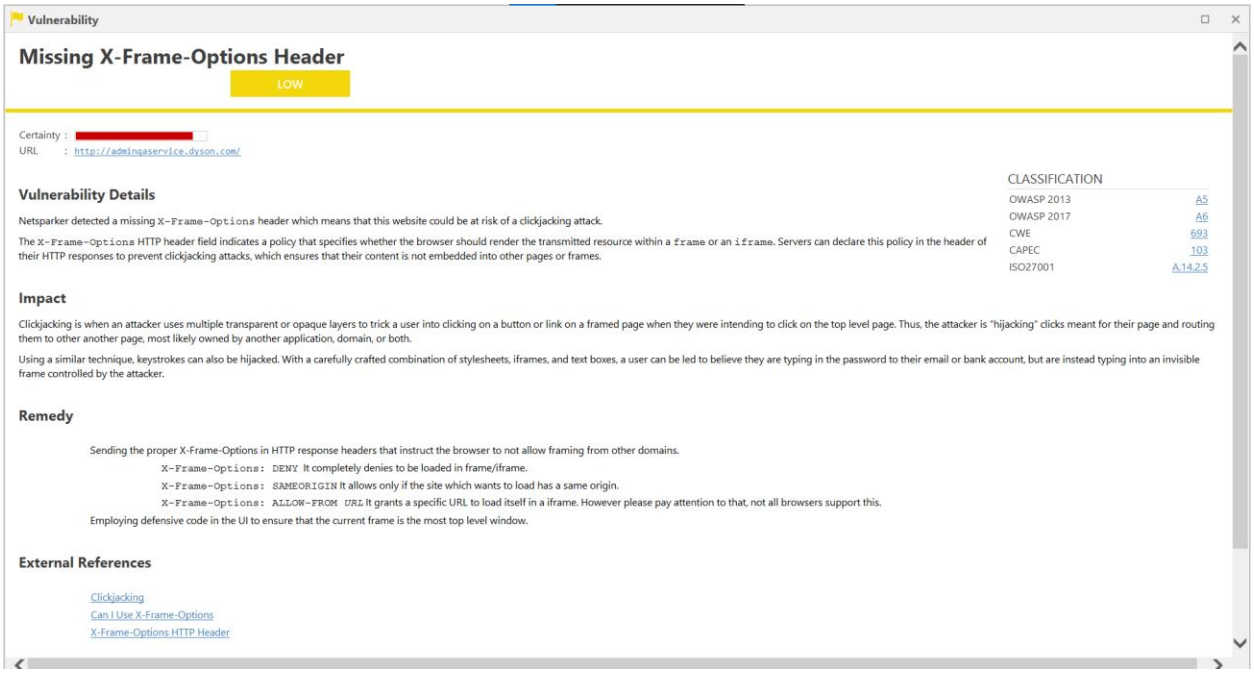
```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln adminqaservice.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-16 22:57 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
------------------ Timing report ------------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:57
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 22:58, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:58
Completed NSE at 22:58, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 22:58
mass_rdns: 0.18s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 22:58, 0.18s elapsed
DNS resolution of 1 IPs took 0.18s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 22:58
Scanning adminqaservice.dyson.com (52.59.125.242) [1000 ports]
Discovered open port 25/tcp on 52.59.125.242
Completed Connect Scan at 22:58, 4.30s elapsed (1000 total ports)
Overall sending rates: 465.63 packets / s.
NSE: Script scanning 52.59.125.242.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:58
NSE: [firewall-bypass] lacks privileges.
NSE: [tls-ticketbleed] Not running due to lack of privileges.
NSE: Starting smtp-vuln-cve2011-1764 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting smtp-vuln-cve2011-1720 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting smtp-vuln-cve2010-4344 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting rsa-vuln-roca against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting ssl-heartbleed against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting http-vuln-cve2014-2129 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting ssl-ccs-injection against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting sslv2-drown against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting ssl-poodle against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting http-vuln-cve2014-2126 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting http-vuln-cve2014-2127 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting ssl-cert-intaddr against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting ssl-dh-params against adminqaservice.dyson.com (52.59.125.242:25).
NSE: Starting http-vuln-cve2014-2128 against adminqaservice.dyson.com (52.59.125.242:25).
NSE: [smtp-vuln-cve2011-1720 52.59.125.242:25] unspecified error
```

```
PORT   STATE SERVICE REASON
25/tcp open  smtp    syn-ack
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
Final times for host: srtt: 13716 rttvar: 11607  to: 100000
```

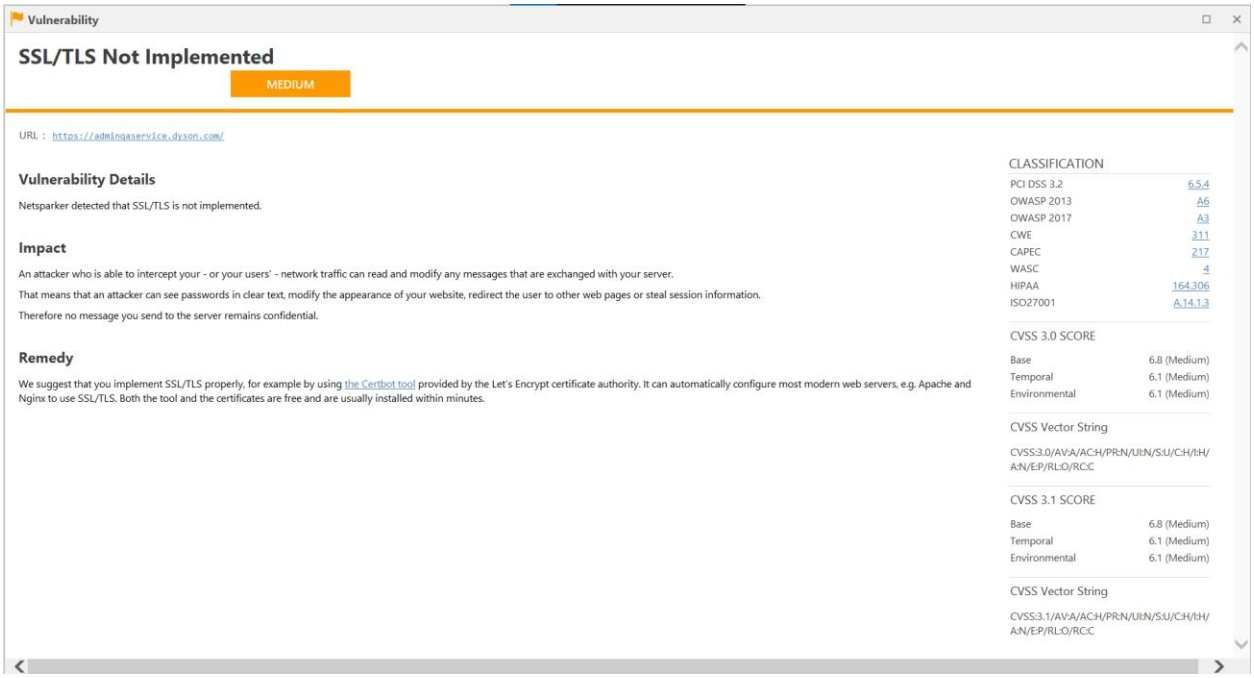
The scan did not detect any other vulnerabilities on port 25.

- **Netsparker**


adminqaservice.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Retest All
Hawk Check
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Post Scan
Scan Session
Tools
Sitemap - Previous Settings
Enter text to search...
adminqaservice.dyson.com:80
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Implem...
Missing X-XSS-Protection Header
Referrer-Policy Not Implemented
adminqaservice.dyson.com:443
SSL/TLS Not Implemented
Issues - Previous Settings
Enter text to search...
adminqaservice.dyson.com:80 (4)
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Implem...
Missing X-XSS-Protection Header
Referrer-Policy Not Implemented
adminqaservice.dyson.com:443 (1)
SSL/TLS Not Implemented
Progress
Scan Speed
Scan Progress
100.00%
Links: 2
Head Requests: 46
Start: 4/20/2024 10:14:23 PM
Failed Requests: 3
Total Requests: 358
404 Responses: 1
Elapsed: 00:01:09
Activity
Progress
Logs (23)
Knowledge Base (7)
Crawling Performance [2]
MIME Types [7]
Not Founds [1]
Out of Scope Links [1]
Scan Performance [35]
Site Profile [1]
Slowest Pages [1]


Vulnerability
Missing X-Frame-Options Header
LOW
Certainty :
URL : http://adminqaservice.dyson.com/
Vulnerability Details
Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.
The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.
CLASSIFICATION
OWASP 2013 A5
OWASP 2017 A6
CWE 693
CAPEC 103
ISO27001 A.14.2.5
Impact
Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.
Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.
Remedy
Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
Employing defensive code in the UI to ensure that the current frame is the most top level window.
External References
Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

Addressing this vulnerability by implementing the X Frame Options header is crucial for protecting the website from clickjacking attacks and ensuring the security of user interactions.



Vulnerability

SSL/TLS Not Implemented

MEDIUM

URL : https://adminqaservice.dyson.com/

Vulnerability Details

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	311
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Addressing this vulnerability by implementing SSL/TLS is crucial for safeguarding the confidentiality and integrity of the website is communication with users and mitigating the risks associated with potential attacks.

Report 04

Target sub domain : api-alexa-login.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h api-alexa-login.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.32.29.11, 96.17.180.45
+ Target IP:          23.32.29.11
+ Target Hostname:    api-alexa-login.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 02:00:19 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: Cookie _abck created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie bm_sz created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; desc="1713333560055_387980551_3124625821_3273_8749_52_0_-";dur=1,).
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://api-alexa-login.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8046 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-04-17 02:15:41 (GMT-4) (922 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Cookie _abck created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

- Cookie bm_sz created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

- The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

- The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u https://api-alexa-login.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ========
This scan has been saved in the file /home/rasan/.wapiti/scans/api-alexa-login.dyson.com_folder_6b8c8e50.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags
Checking cookie : _abck
HttpOnly flag is not set in the cookie : _abck
Checking cookie : bm_sz
HttpOnly flag is not set in the cookie : bm_sz
Secure flag is not set in the cookie : bm_sz
Checking cookie : ak_bmsc
HttpOnly flag is not set in the cookie : ak_bmsc
Secure flag is not set in the cookie : ak_bmsc
Checking cookie : bm_sv
HttpOnly flag is not set in the cookie : bm_sv

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=27b23u for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
------
A report has been generated in the file /home/rasan/.wapiti/generated_report
Open /home/rasan/.wapiti/generated_report/api-alexa-login.dyson.com_04172024_0602.html with a browser to see this report.
```

Wapiti vulnerability report

Target: https://api-alexa-login.dyson.com/

Date of the scan: Wed, 17 Apr 2024 06:02:24 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	2
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

- **HTTP secure header**

Vulnerabilities

```
o   X-Frame-Options is not set
o   X-XSS-Protection is not set
o   X-Content-Type-Options is not set
o   Strict-Transport-Security is not set
```

Solutions

Use the recommendations for hardening your HTTP Security Headers.

- **HttpOnly Flag cookies**

HttpOnly is an additional flag included in a Set Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client-side script accessing the protected cookie.

Vulnerabilities

```
o   HttpOnly flag is not set in the cookie : _abck
o   HttpOnly flag is not set in the cookie : bm_sz
o   HttpOnly flag is not set in the cookie : ak_bmsc
o   HttpOnly flag is not set in the cookie : bm_sv
```

Solutions

While creation of the cookie make sure to set the HttpOnly Flag to True.

- **Secure Flag cookies**

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text.

Vulnerabilities

- Secure flag is not set in the cookie : bm_sz
- Secure flag is not set in the cookie : ak_bmsc

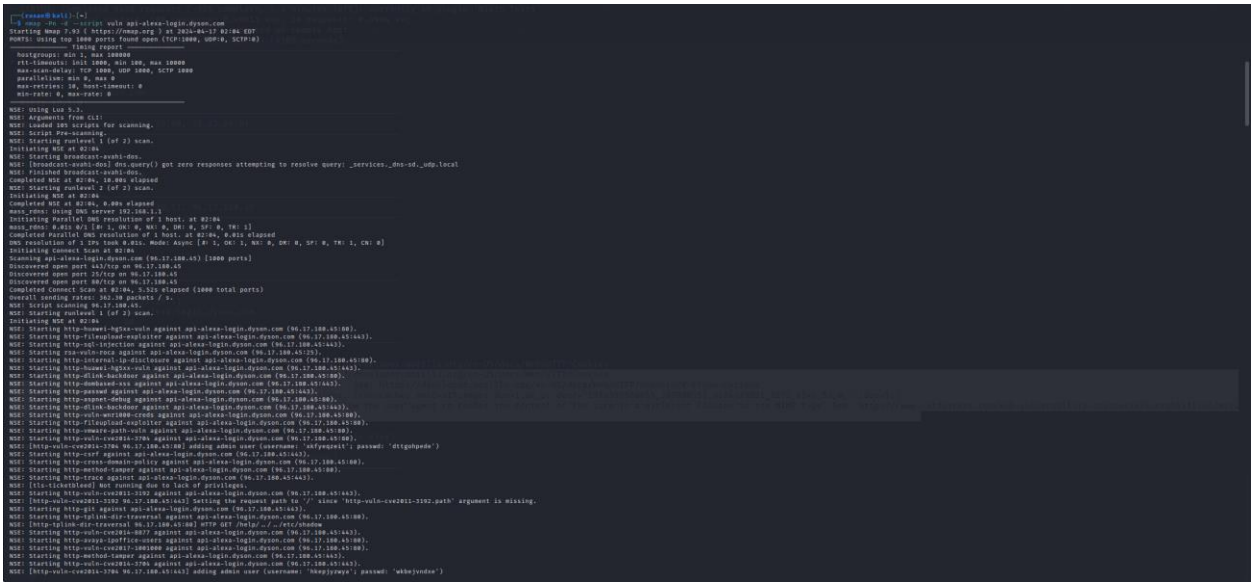
Solutions

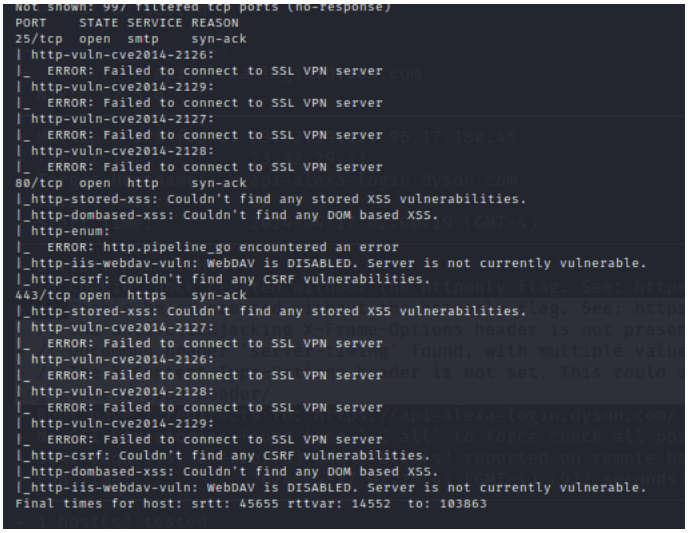
When generating the cookie, make sure to set the Secure Flag to True.

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 api-alexa-login.dyson.com
WhatWeb report for http://api-alexa-login.dyson.com/
Status    : 403 Forbidden
Title     : Access Denied
IP        : 23.32.29.11
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost], UncommonHeaders[server-timing]

Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website     : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String      : AkamaiGHost (from server string)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String      : server-timing (from headers)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 385
        Expires: Wed, 17 Apr 2024 06:33:49 GMT
        Date: Wed, 17 Apr 2024 06:33:49 GMT
        Connection: close
        Server-Timing: cdn-cache; desc=HIT
        Server-Timing: edge; dur=1
        Server-Timing: ak_p; desc="1713335629277_387980551_3144276496_15_5337_241_0_-";dur=1
```

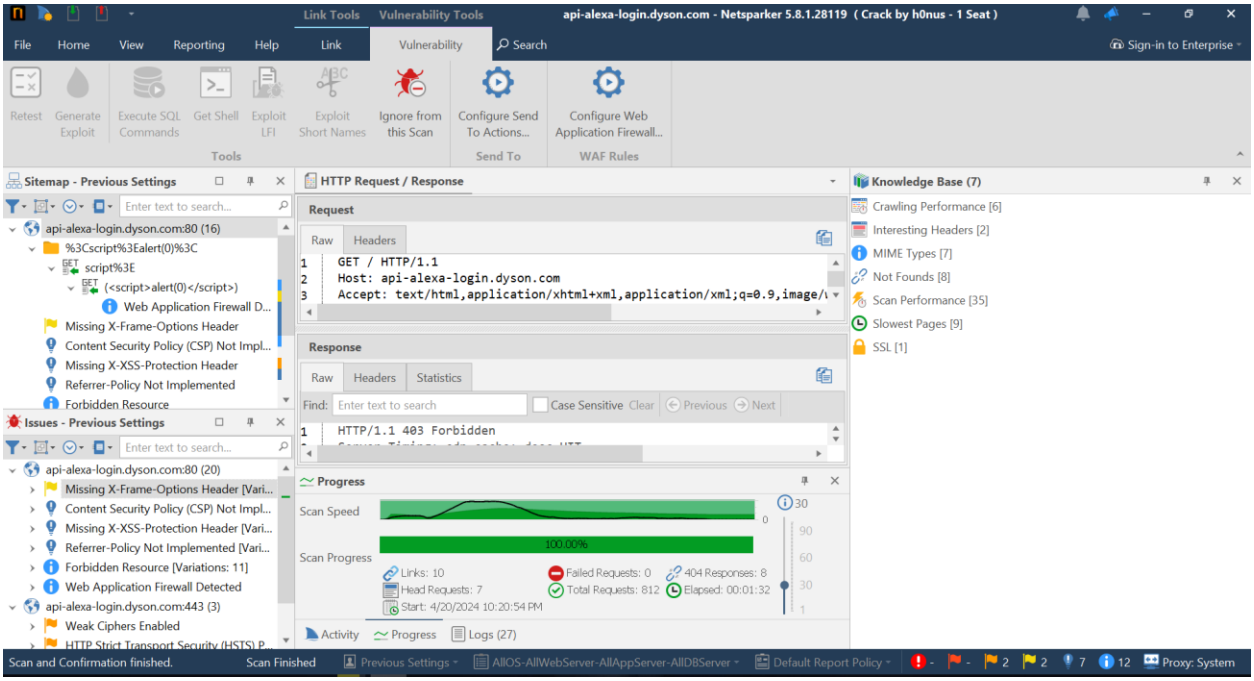
- **Nmap**

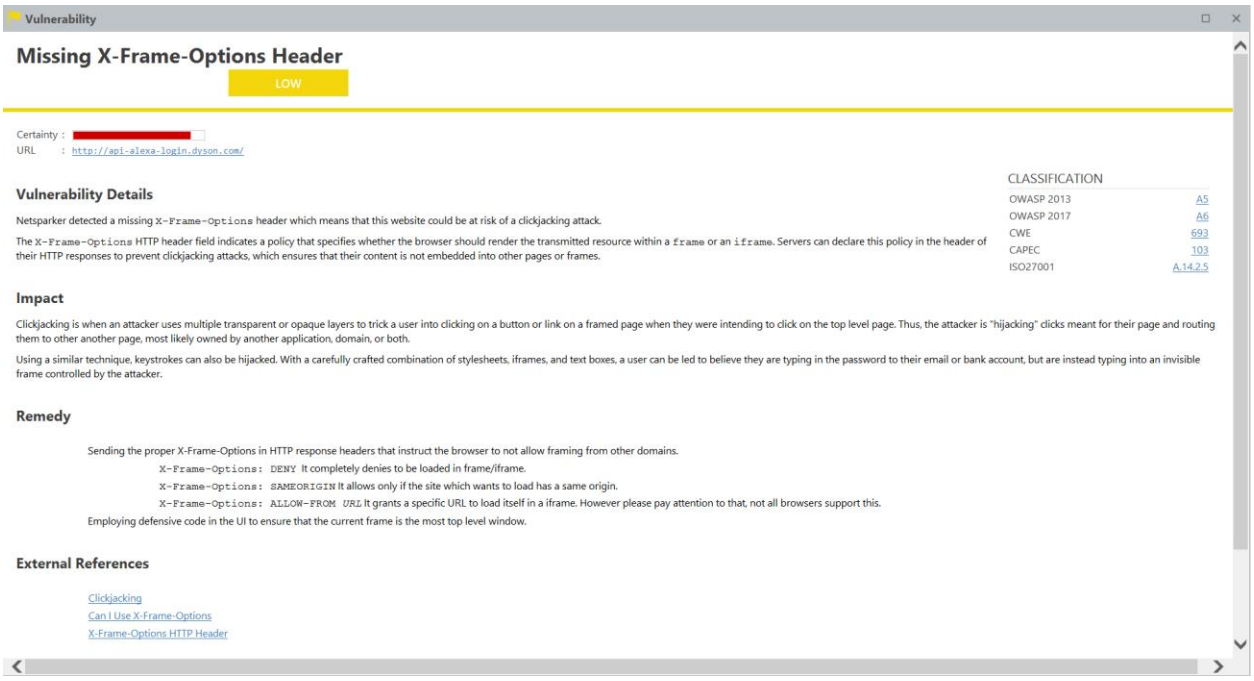




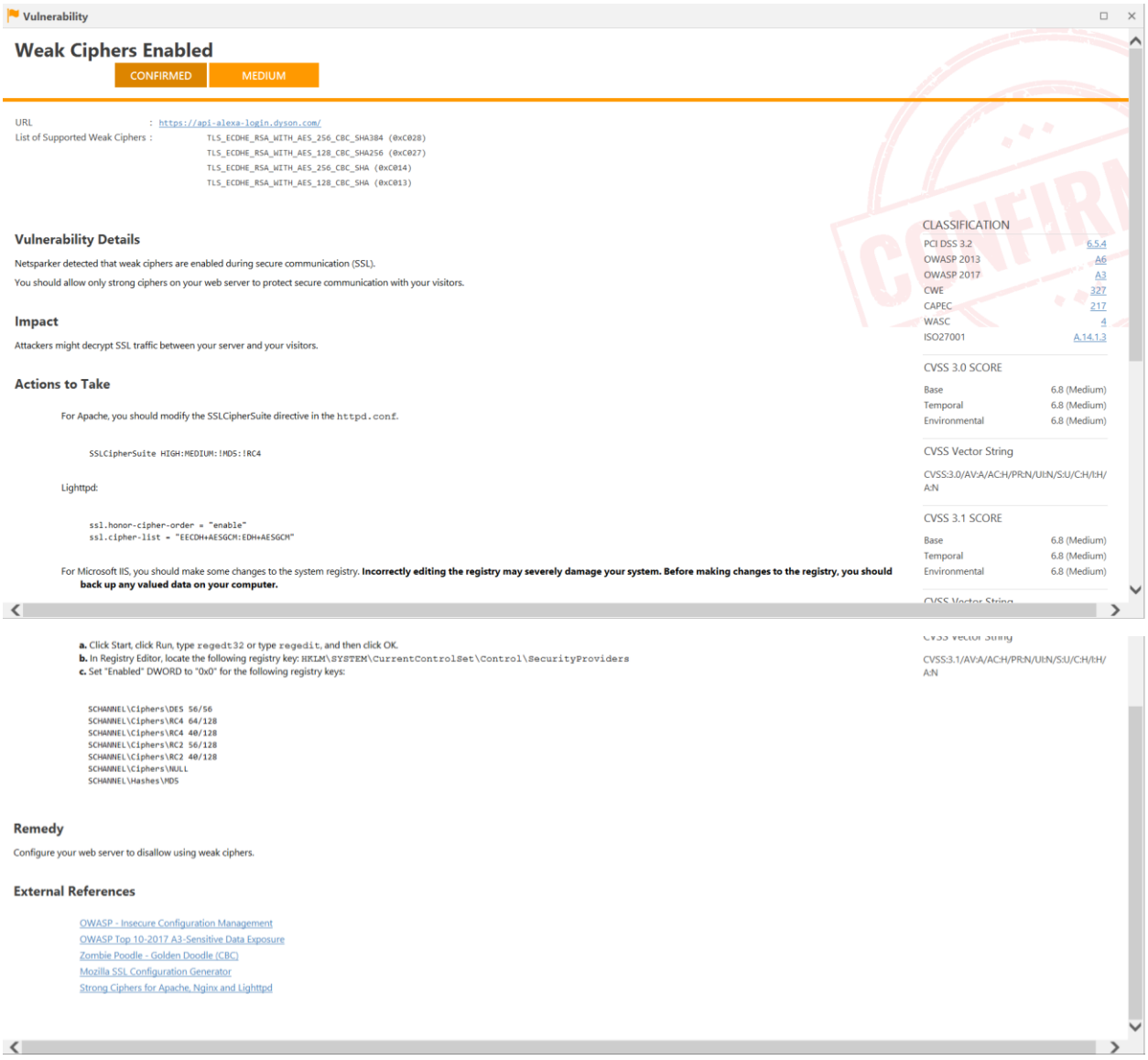
the scan did not detect any vulnerabilities

- **Netsparker**


api-alexa-login.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
Sitemap - Previous Settings
HTTP Request / Response
Knowledge Base (7)
Request
GET / HTTP/1.1
Host: api-alexa-login.dyson.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Response
HTTP/1.1 403 Forbidden
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Missing X-XSS-Protection Header
Referrer-Policy Not Implemented
Forbidden Resource
Issues - Previous Settings
Missing X-Frame-Options Header [Vari...
Forbidden Resource [Variations: 11]
Web Application Firewall Detected
Weak Ciphers Enabled
Progress
Scan Speed
Scan Progress
100.00%
Scan and Confirmation finished.
Scan Finished


Vulnerability
Missing X-Frame-Options Header
LOW
Certainty :
URL : http://api-alexa-login.dyson.com/
Vulnerability Details
Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.
The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.
CLASSIFICATION
OWASP 2013 A5
OWASP 2017 A6
CWE 693
CAPEC 103
ISO27001 A.14.2.5
Impact
Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.
Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.
Remedy
Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
Employing defensive code in the UI to ensure that the current frame is the most top level window.
External References
Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

Addressing this vulnerability by implementing the X-Frame-Options header is crucial for protecting the website from clickjacking attacks and ensuring the security of user interactions.



Vulnerability

Weak Ciphers Enabled

CONFIRMED MEDIUM

URL : https://api-alexa-login.dyson.com/

List of Supported Weak Ciphers :
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)

Vulnerability Details

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Addressing this vulnerability by disallowing the use of weak ciphers is crucial for enhancing the security of SSL communication and mitigating the risk of decryption attacks by malicious actors.

Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :
URL : https://api-alexa-login.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
```

Addressing this vulnerability by implementing HSTS policy and redirecting HTTP traffic to HTTPS is crucial for enhancing the security of web communication and mitigating the risk of various attacks.

Report 05

Target sub domain : www.careers.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h www.careers.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 96.17.180.44, 96.17.180.50
+ Target IP:          96.17.180.44
+ Target Hostname:    www.careers.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 02:39:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: Cookie _abck created without the httponly flag. See: https://developer.mozilla.org/en-US/doc
s/Web/HTTP/Cookies
+ /: Cookie bm_sz created without the httponly flag. See: https://developer.mozilla.org/en-US/doc
s/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.
org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-
vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://careers.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8158 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2024-04-17 02:55:46 (GMT-4) (1004 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Cookie _abck created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- Cookie bm_sz created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u https://careers.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ————————
This scan has been saved in the file /home/rasan/.wapiti/scans/careers.dyson.com_folder_6e74c757.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=trq95i for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
————————
A report has been generated in the file /home/rasan/.wapiti/generated_report
Open /home/rasan/.wapiti/generated_report/careers.dyson.com_04172024_1628.html with a browser to see this report.
```

Wapiti vulnerability report

Target: https://careers.dyson.com/

Date of the scan: Wed, 17 Apr 2024 16:28:42 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

➢ **HTTP secure headers**

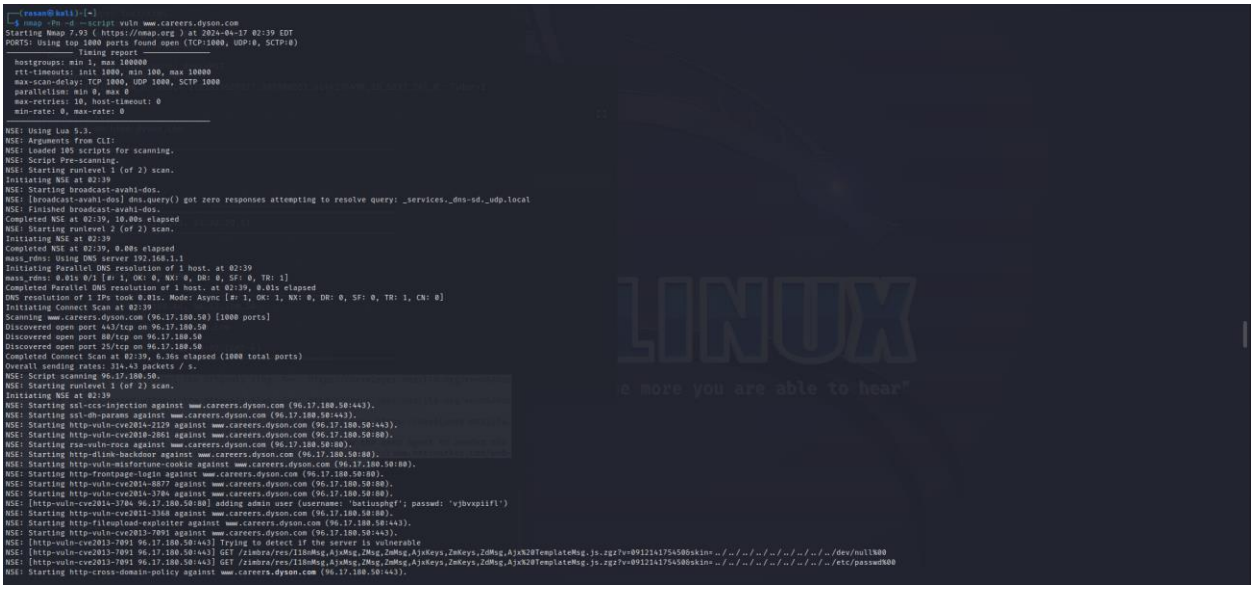
Vulnerability

- X-Frame-Options is not set
- X-XSS-Protection is not set
- X-Content-Type-Options is not set
- Strict-Transport-Security is not set

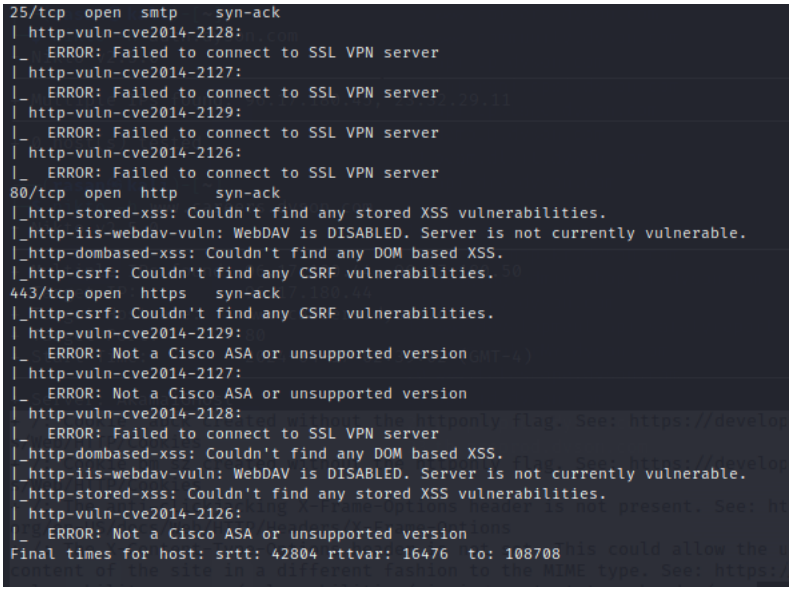
- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 careers.dyson.com
WhatWeb report for http://careers.dyson.com
Status    : 403 Forbidden
Title     : Access Denied
IP        : 23.32.29.98
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost]

Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website     : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : AkamaiGHost (from server string)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 371
        Expires: Wed, 17 Apr 2024 16:36:01 GMT
        Date: Wed, 17 Apr 2024 16:36:01 GMT
        Connection: close
```

- **Nmap**



```
┌──(reasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln www.careers.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 02:39 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
                 ------------------ Timing report ------------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 02:39
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 02:39, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 02:39
Completed NSE at 02:39, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 02:39
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 02:39, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 02:39
Scanning www.careers.dyson.com (96.17.180.50) [1000 ports]
Discovered open port 443/tcp on 96.17.180.50
Discovered open port 80/tcp on 96.17.180.50
Discovered open port 25/tcp on 96.17.180.50
Completed Connect Scan at 02:39, 6.36s elapsed (1000 total ports)
Overall sending rates: 314.43 packets / s.
NSE: Script scanning 96.17.180.50.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 02:39
NSE: Starting ssl-ccs-injection against www.careers.dyson.com (96.17.180.50:443).
NSE: Starting ssl-dh-params against www.careers.dyson.com (96.17.180.50:443).
NSE: Starting http-vuln-cve2014-2129 against www.careers.dyson.com (96.17.180.50:443).
NSE: Starting http-vuln-cve2010-2861 against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting rsa-vuln-roca against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting http-dlink-backdoor against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting http-vuln-misfortune-cookie against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting http-frontpage-login against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting http-vuln-cve2014-8877 against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting http-vuln-cve2014-3704 against www.careers.dyson.com (96.17.180.50:80).
NSE: [http-vuln-cve2014-3704 96.17.180.50:80] adding admin user {username: 'batiuspqgf'; passwd: 'wjbvxpiifl'}
NSE: Starting http-vuln-cve2011-3368 against www.careers.dyson.com (96.17.180.50:80).
NSE: Starting http-fileupload-exploiter against www.careers.dyson.com (96.17.180.50:443).
NSE: Starting http-vuln-cve2013-7091 against www.careers.dyson.com (96.17.180.50:443).
NSE: [http-vuln-cve2013-7091 96.17.180.50:443] Trying to detect if the server is vulnerable
NSE: [http-vuln-cve2013-7091 96.17.180.50:443] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../../../../../dev/null%00
NSE: [http-vuln-cve2013-7091 96.17.180.50:443] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../../../../../etc/passwd%00
NSE: Starting http-cross-domain-policy against www.careers.dyson.com (96.17.180.50:443).
```

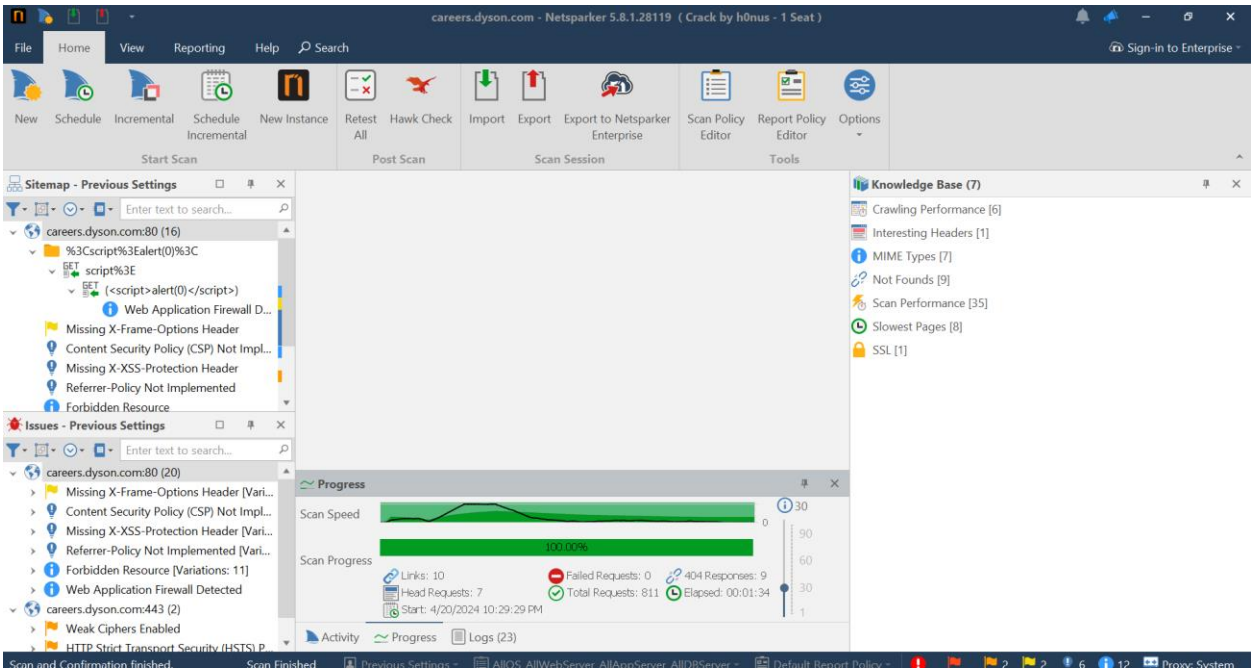


```
25/tcp  open  smtp    syn-ack
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
80/tcp  open  http    syn-ack
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open  https   syn-ack
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-vuln-cve2014-2129:
|_  ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2127:
|_  ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2014-2126:
|_  ERROR: Not a Cisco ASA or unsupported version
Final times for host: srtt: 42804 rttvar: 16476  to: 108708
```

- Port 25 (SMTP): No specific vulnerabilities were tested or reported for this port.
- Port 80 (HTTP): No vulnerabilities detected.

- Port 443 (HTTPS): No vulnerabilities detected, except for errors related to CVE-2014-2126, CVE-2014-2127, CVE-2014-2128, and CVE-2014-2129, which were not exploitable.

- **Netsparker**



Vulnerability

Missing X-Frame-Options Header

LOW

Certainty :
URL : http://careers.dyson.com/

Vulnerability Details

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

- `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
- `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
- `X-Frame-Options: ALLOW-FROM URL` It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

Addressing this vulnerability by implementing the X-Frame-Options header is crucial for protecting the website from clickjacking attacks and ensuring the security of user interactions.

Vulnerability

Weak Ciphers Enabled

CONFIRMED MEDIUM

URL : https://careers.dyson.com/
List of Supported Weak Ciphers :
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)

Vulnerability Details

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

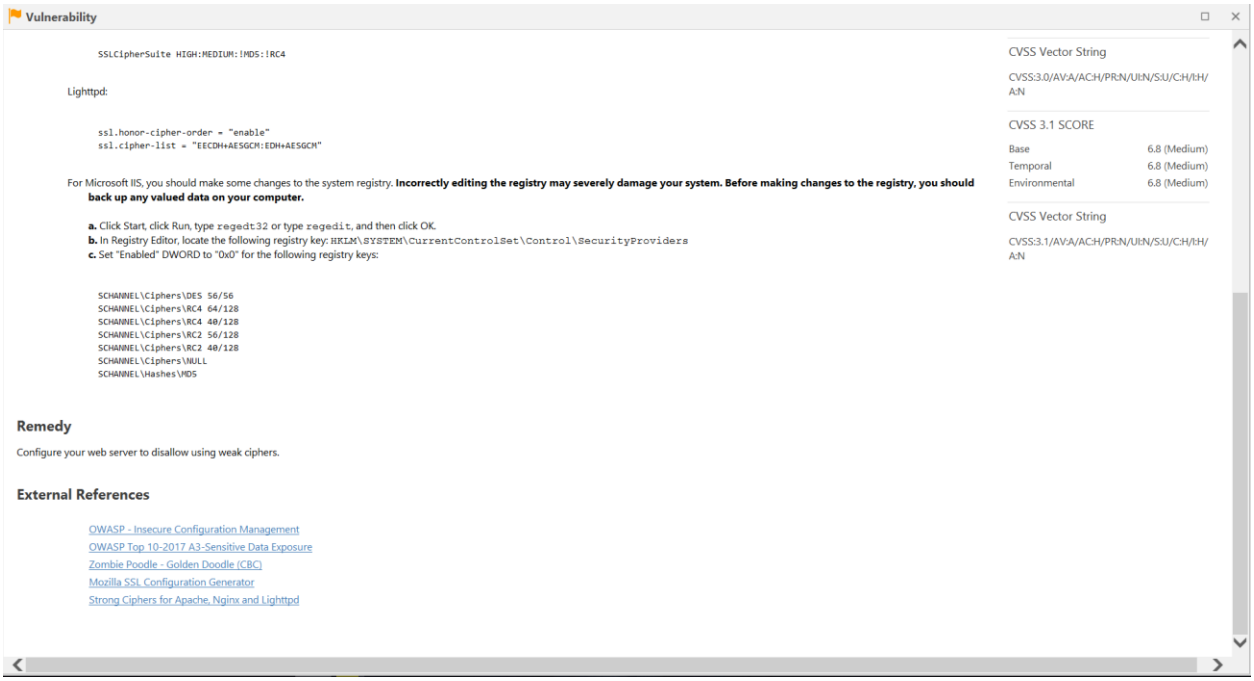
Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.



Vulnerability

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedit32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

addressing this vulnerability by disallowing the use of weak ciphers is crucial for enhancing the security of SSL communication and mitigating the risk of decryption attacks by malicious actors.

Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :
URL : https://careers.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
```

Addressing this vulnerability by implementing HSTS policy and redirecting HTTP traffic to HTTPS is crucial for enhancing the security of web communication and mitigating the risk of various attacks.

Report 06

Target sub domain : api.cp.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h api.cp.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.204.15, 104.18.205.15
+ Target IP:          104.18.204.15
+ Target Hostname:    api.cp.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 12:38:36 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 26608 requests: 4 error(s) and 3 item(s) reported on remote host
+ End Time:         2024-04-17 12:52:50 (GMT-4) (854 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on these findings, there are a couple of potential vulnerabilities and security issues to address

- The absence of the X-Content-Type-Options header could lead to MIME type sniffing attacks.
- Publicly accessible CGI directories might expose CGI scripts to vulnerabilities.

  When CGI (Common Gateway Interface) directories are publicly accessible it means that anyone on the internet can potentially access and interact with the CGI scripts stored within those directories. This could lead to vulnerabilities if the scripts are not properly secured or if there are flaws in their implementation. Attackers may exploit these vulnerabilities to gain unauthorized access to the system, execute arbitrary code or perform other malicious actions.
- The presence of Cloudflare trace CGI could potentially leak system information

  Cloudflare trace CGI is a feature that allows users to trace the route from Cloudflare to the origin server. However if this feature is misconfigured or improperly secured it could potentially leak sensitive system information such as server configurations or internal network details. This could provide attackers with valuable insights into the system architecture making it easier for them to launch targeted attacks

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u http://api.cp.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ────
This scan has been saved in the file /home/rasan/.wapiti/scans/api.cp.dyson.com_folder_68ae228c.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
OK
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=xw4p2c for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

 Report
 ──────
A report has been generated in the file /home/rasan/.wapiti/generated_report
Open /home/rasan/.wapiti/generated_report/api.cp.dyson.com_04172024_1649.html with a browser to see this report.
```

Wapiti vulnerability report

Target: http://api.cp.dyson.com/

Date of the scan: Wed, 17 Apr 2024 16:49:36 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	3
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0

SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-XSS-Protection is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Content-Type-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
Strict-Transport-Security is not set
```

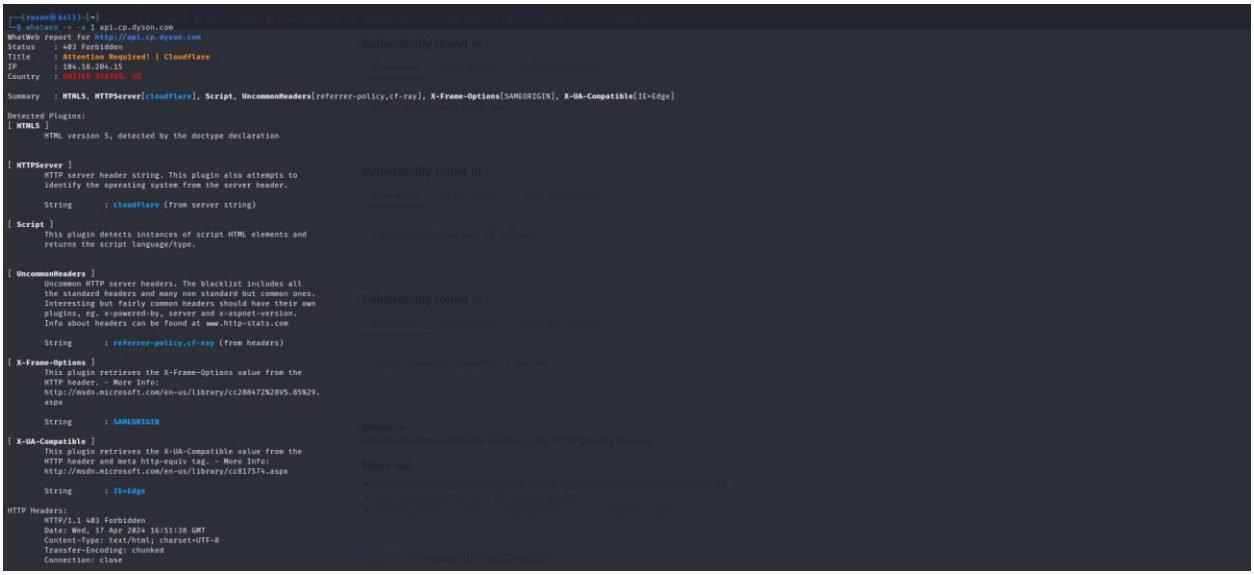
Solutions

Use the recommendations for hardening your HTTP Security Headers.

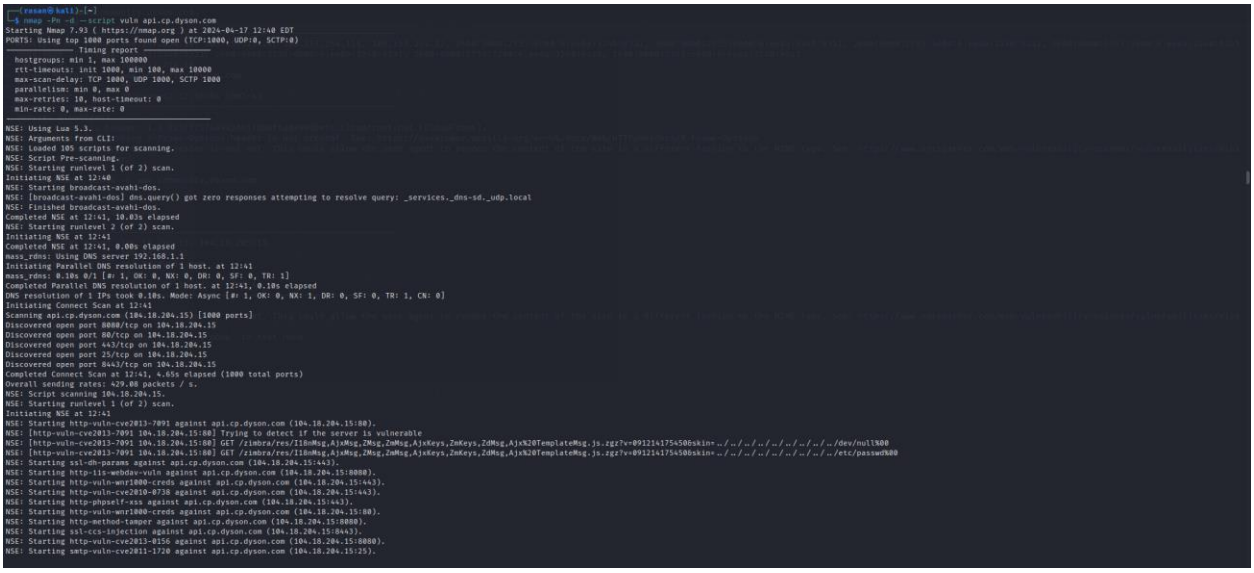
References

- Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications
- KeyCDN: Hardening Your HTTP Security Headers
- OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)

- **Whatweb**



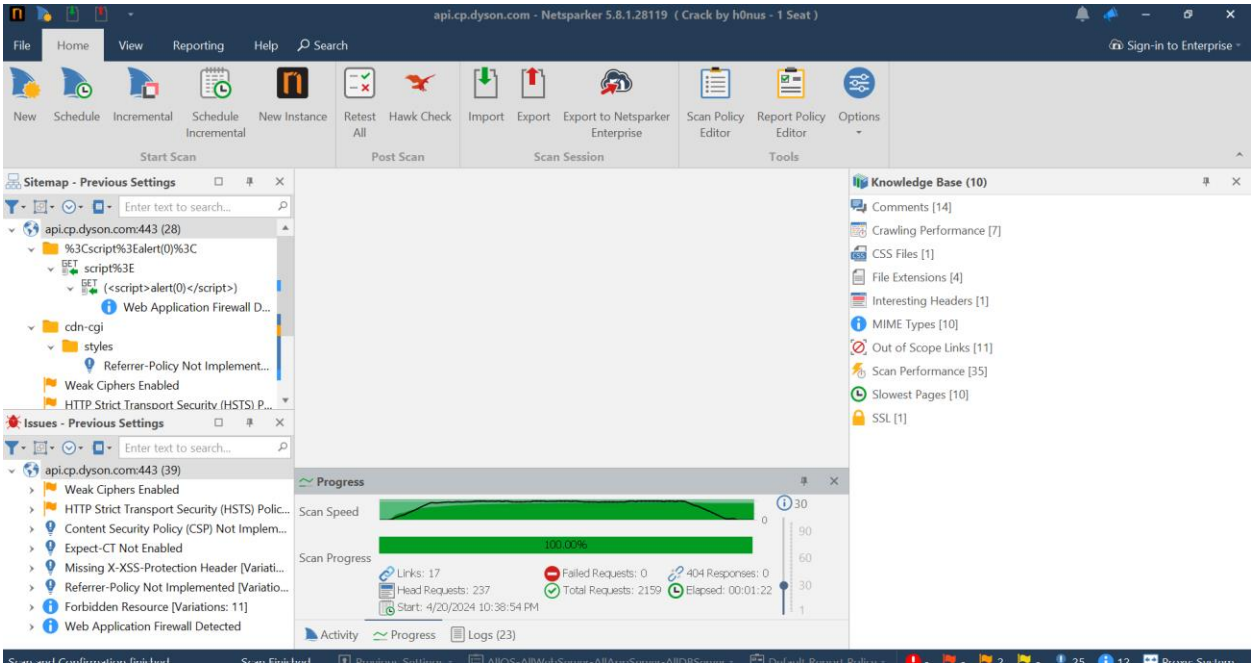
- **Nmap**

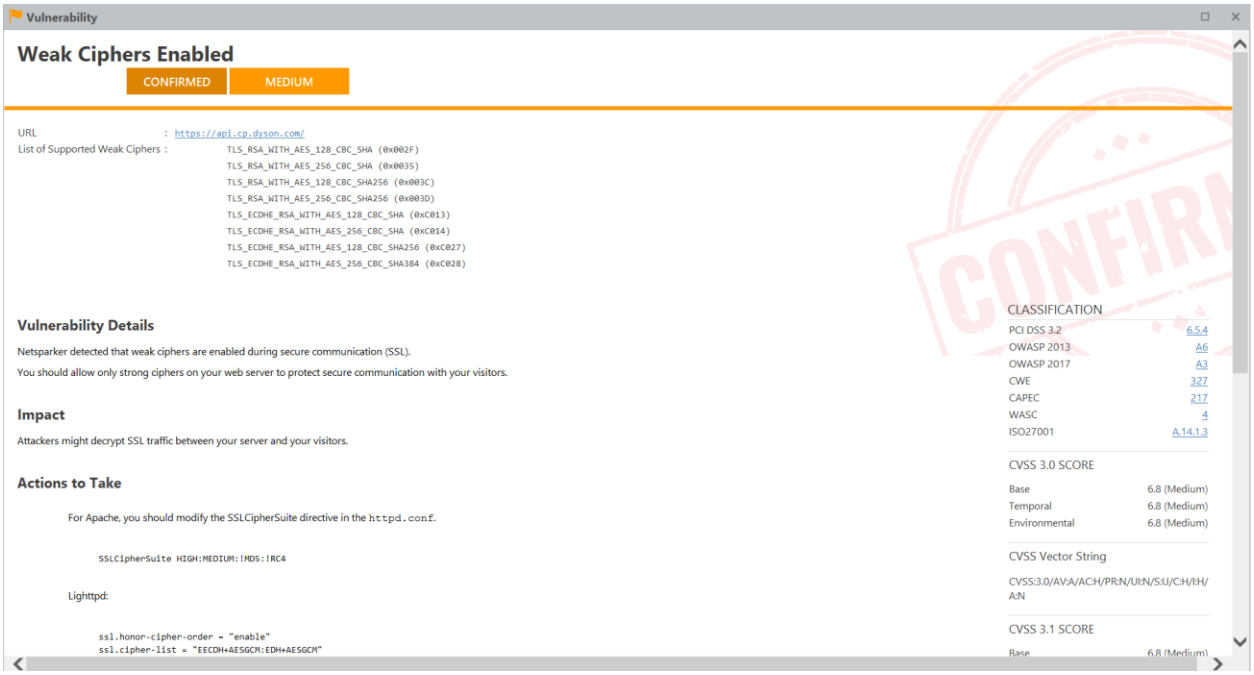


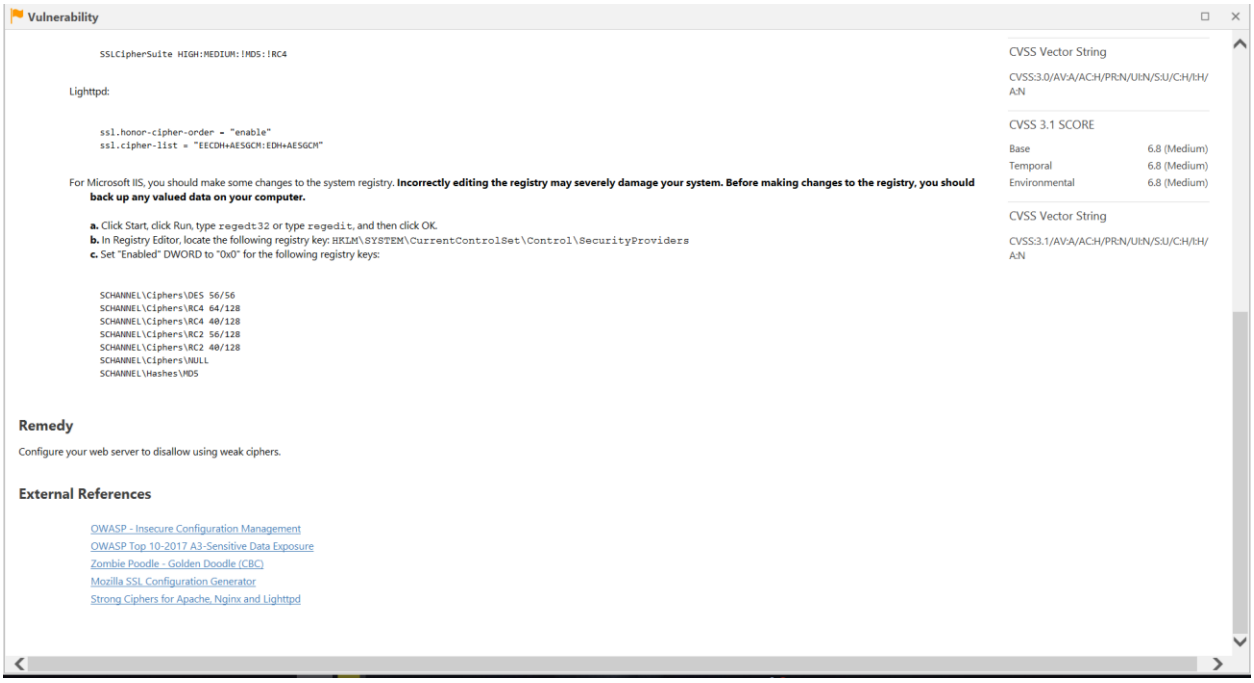
```
PORT     STATE SERVICE    REASON
25/tcp   open  smtp       syn-ack
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
80/tcp   open  http       syn-ack
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-iis-webdav-vuln:
|_  ERROR: This web server is not supported.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp  open  https      syn-ack
| http-iis-webdav-vuln:
|_  ERROR: This web server is not supported.
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
8080/tcp open  http-proxy syn-ack
| http-iis-webdav-vuln:
|_  ERROR: This web server is not supported.
8443/tcp open  https-alt  syn-ack
| http-iis-webdav-vuln:
|_  ERROR: This web server is not supported.
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
Final times for host: srtt: 13992 rttvar: 7662  to: 100000
```

Zero vulnerabilities found.

- **Netsparker**


api.cp.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Retest All
Hawk Check
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Post Scan
Scan Session
Tools
Sitemap - Previous Settings
Enter text to search...
api.cp.dyson.com:443 (28)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
cdn-cgi
styles
Referrer-Policy Not Implement...
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Issues - Previous Settings
Enter text to search...
api.cp.dyson.com:443 (39)
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) Polic...
Content Security Policy (CSP) Not Implem...
Expect-CT Not Enabled
Missing X-XSS-Protection Header [Variati...
Referrer-Policy Not Implemented [Variatio...
Forbidden Resource [Variations: 11]
Web Application Firewall Detected
Progress
Scan Speed
Scan Progress
100.00%
Links: 17
Head Requests: 237
Start: 4/20/2024 10:38:54 PM
Failed Requests: 0
Total Requests: 2159
404 Responses: 0
Elapsed: 00:01:22
Activity
Progress
Logs (23)
Knowledge Base (10)
Comments [14]
Crawling Performance [7]
CSS Files [1]
File Extensions [4]
Interesting Headers [1]
MIME Types [10]
Out of Scope Links [11]
Scan Performance [35]
Slowest Pages [10]
SSL [1]


Vulnerability
Weak Ciphers Enabled
CONFIRMED
MEDIUM
URL : https://api.cp.dyson.com/
List of Supported Weak Ciphers :
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
Vulnerability Details
Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Impact
Attackers might decrypt SSL traffic between your server and your visitors.
Actions to Take
For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
Lighttpd:
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
CLASSIFICATION
PCI DSS 3.2 6.5.4
OWASP 2013 A6
OWASP 2017 A3
CWE 327
CAPEC 217
WASC 4
ISO27001 A.14.1.3
CVSS 3.0 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)
CVSS Vector String
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
CVSS 3.1 SCORE



Vulnerability

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Addressing this vulnerability by disallowing the use of weak ciphers is crucial for enhancing the security of SSL communication and mitigating the risk of decryption attacks by malicious actors.

Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :
URL : https://api.cp.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
```

Vulnerability

server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

Wikipedia - HTTP Strict Transport Security
Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
HTTP Strict Transport Security (HSTS) HTTP Header
Mozilla SSL Configuration Generator

addressing this vulnerability by implementing HSTS policy and redirecting HTTP traffic to HTTPS is crucial for enhancing the security of web communication and mitigating the risk of various attacks.

Report 07

Target sub domain : api.cpstage.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h api.cpstage.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 52.59.122.122, 52.59.125.242
+ Target IP:          52.59.122.122
+ Target Hostname:    api.cpstage.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 22:10:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/
Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
 different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-co
ntent-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2024-04-17 23:10:39 (GMT-4) (3589 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on the findings there are a couple of vulnerabilities and security concerns to address

- The absence of the X-Frame-Options header leaves the site susceptible to clickjacking attacks.
- The lack of the X-Content-Type-Options header could lead to MIME type sniffing attacks.

- **Wapiti**

Wapiti vulnerability report
Target: https://api.cpstage.dyson.com/
Date of the scan: Thu, 18 Apr 2024 02:12:54 +0000. Scope of the scan: folder

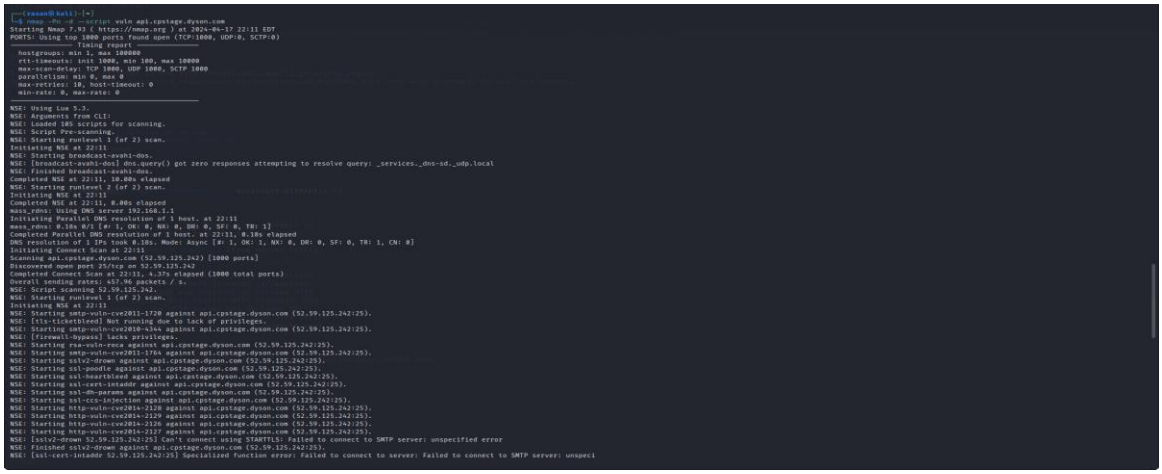
Summary

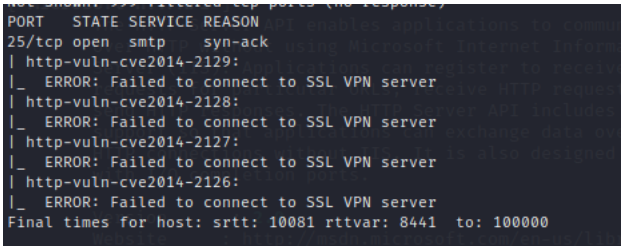
Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	0
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	0
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 api.cpstage.dyson.com
WhatWeb report for http://api.cpstage.dyson.com
Status    : 404 Not Found
Title     : Not Found
IP        : 52.59.122.122
Country   : UNITED STATES, US

Summary   : HTTPServer[Microsoft-HTTPAPI/2.0], Microsoft-HTTPAPI[2.0]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-HTTPAPI/2.0 (from server string)

[ Microsoft-HTTPAPI ]
        The HTTP Server API enables applications to communicate
        over HTTP without using Microsoft Internet Information
        Server (IIS). Applications can register to receive HTTP
        requests for particular URLs, receive HTTP requests, and
        send HTTP responses. The HTTP Server API includes SSL
        support so that applications can exchange data over secure
        HTTP connections without IIS. It is also designed to work
        with I/O completion ports.

        Version      : 2.0
        Website     : http://msdn.microsoft.com/en-us/library/aa364510%28v=vs.85%29.aspx

HTTP Headers:
        HTTP/1.1 404 Not Found
        Content-Type: text/html; charset=us-ascii
        Server: Microsoft-HTTPAPI/2.0
        Date: Thu, 18 Apr 2024 02:15:40 GMT
        Connection: close
        Content-Length: 315
```

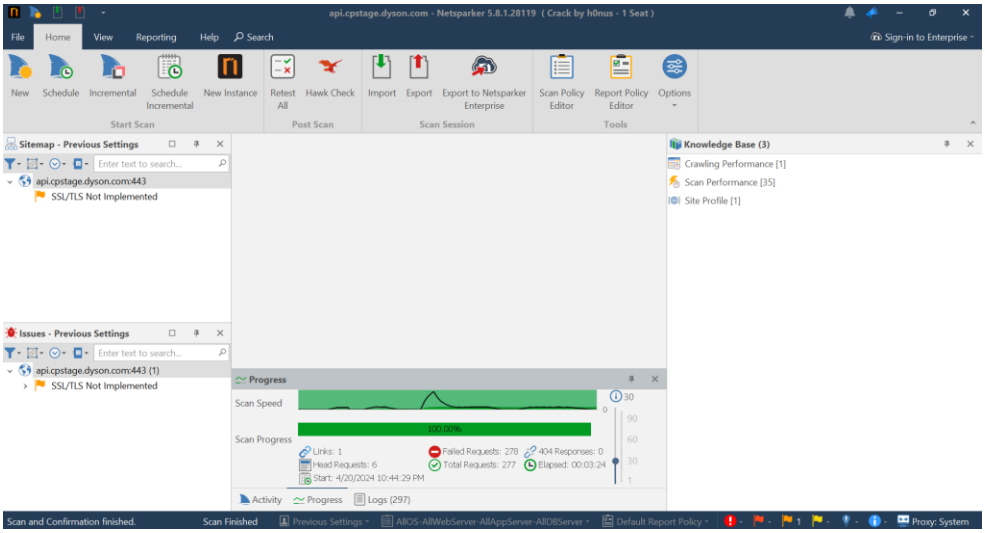
- **Nmap**

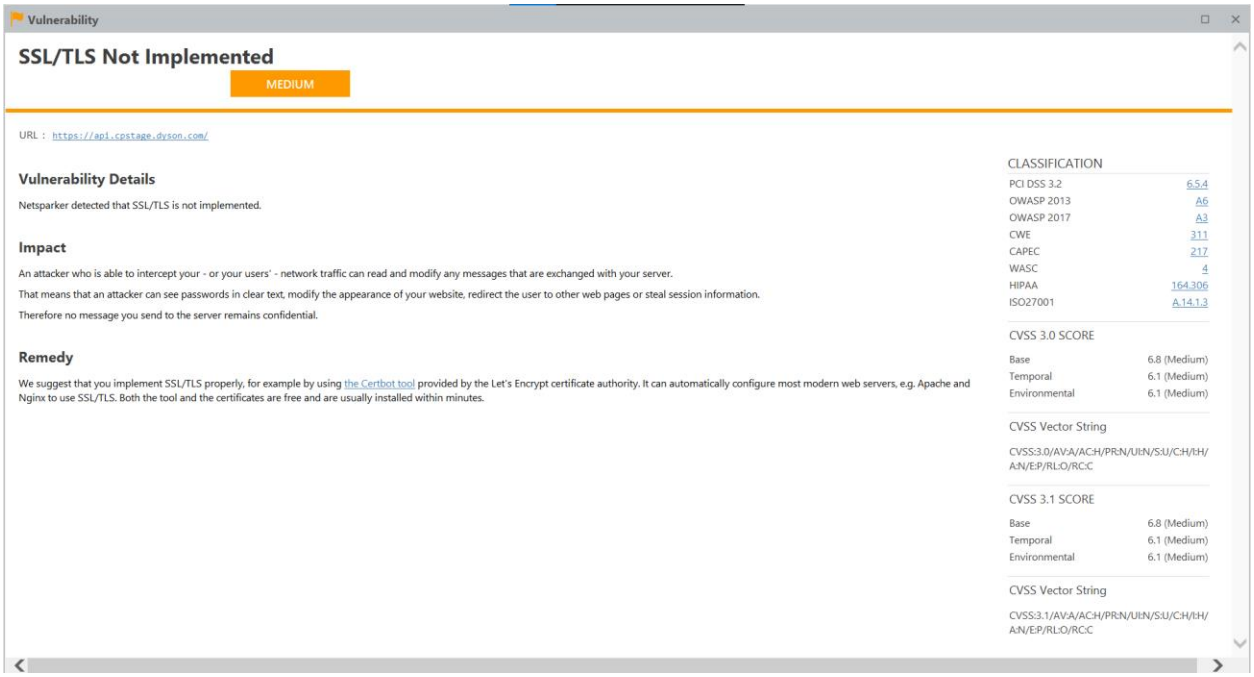




Zero vulnerabilities found

- **Netsparker**





Vulnerability

SSL/TLS Not Implemented

MEDIUM

URL : https://api.cpstage.dyson.com/

Vulnerability Details

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	311
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Addressing this vulnerability by implementing SSL/TLS is crucial for ensuring the security of data transmitted between the server and users and mitigating the risk of interception and manipulation by attackers

Report 08

Target sub domain : demo3D.dyson.com

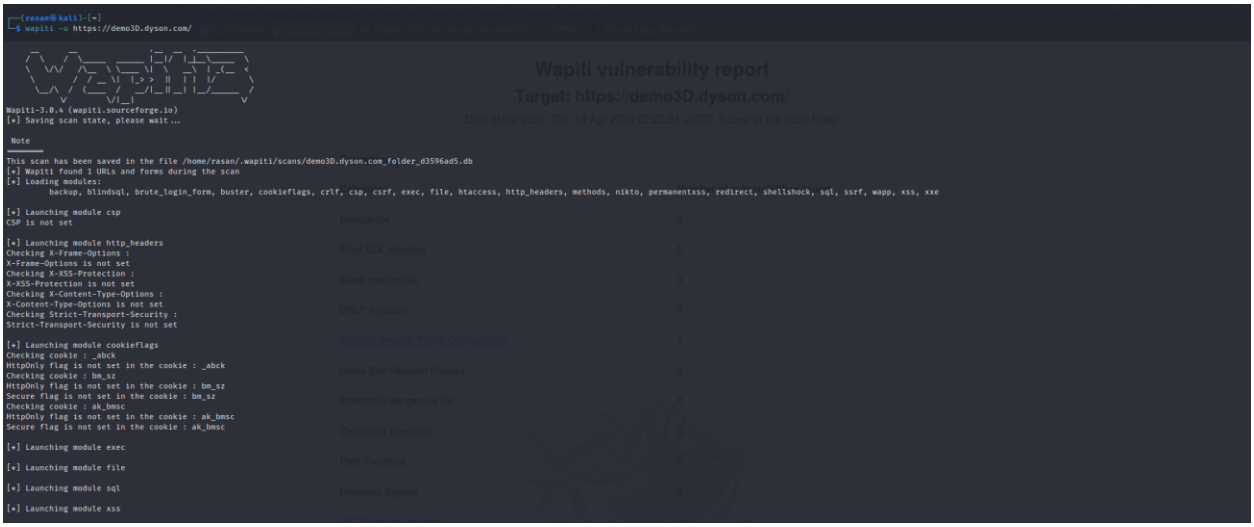
- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h demo3D.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.215.7.29, 23.215.7.26
+ Target IP:          23.215.7.29
+ Target Hostname:    demo3D.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 22:20:54 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: Cookie _abck created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie bm_sz created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://demo3d.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'AkamaiGHost' to 'CloudFront'.
+ 8046 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-04-17 22:34:24 (GMT-4) (810 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on these findings there are a few vulnerabilities and security concerns to address

- Cookies created without the httponly flag could be vulnerable to client-side attacks.
- The absence of the X-Frame-Options header leaves the site susceptible to clickjacking attacks.
- The lack of the X-Content-Type-Options header could lead to MIME type sniffing attacks.
- The server banner changed during the scan which might indicate changes in the server configuration.

- **Wapiti**



```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u https://demo3D.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[+] Saving scan state, please wait ...

 Note
 ----
This scan has been saved in the file /home/rasan/.wapiti/scans/demo3D.dyson.com_folder_d3596ad5.db
[+] Wapiti found 1 URLs and forms during the scan
[+] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[+] Launching module csp
CSP is not set

[+] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[+] Launching module cookieflags
Checking cookie : _abck
HttpOnly flag is not set in the cookie : _abck
Checking cookie : bm_sz
HttpOnly flag is not set in the cookie : bm_sz
Secure flag is not set in the cookie : bm_sz
Checking cookie : ak_bmsc
HttpOnly flag is not set in the cookie : ak_bmsc
Secure flag is not set in the cookie : ak_bmsc

[+] Launching module exec

[+] Launching module file

[+] Launching module sql

[+] Launching module xss
```

Wapiti vulnerability report

Target: https://demo3D.dyson.com/

Date of the scan: Thu, 18 Apr 2024 02:23:31 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	2
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Frame-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-XSS-Protection is not set
```

Vulnerability found in /

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Content-Type-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
Strict-Transport-Security is not set
```

Solutions

Use the recommendations for hardening your HTTP Security Headers.

References

- Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications
- KeyCDN: Hardening Your HTTP Security Headers
- OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)

HttpOnly Flag cookie

Description

HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie (if the browser supports it).

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : _abck
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : bm_sz
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : ak_bmsc
```

Solutions

While creation of the cookie, make sure to set the HttpOnly Flag to True.

References

- OWASP: Testing for Cookies Attributes
- OWASP: HttpOnly

Secure Flag cookie

Description

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
Secure flag is not set in the cookie : bm_sz
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
Secure flag is not set in the cookie : ak_bmsc
```

Solutions

When generating the cookie, make sure to set the Secure Flag to True.

References

- OWASP: Testing for Cookies Attributes

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 demo3D.dyson.com
WhatWeb report for http://demo3D.dyson.com
Status    : 403 Forbidden
Title     : Access Denied
IP        : 96.17.180.45
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost]

Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website     : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String      : AkamaiGHost (from server string)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 368
        Expires: Thu, 18 Apr 2024 02:27:28 GMT
        Date: Thu, 18 Apr 2024 02:27:28 GMT
        Connection: close
```

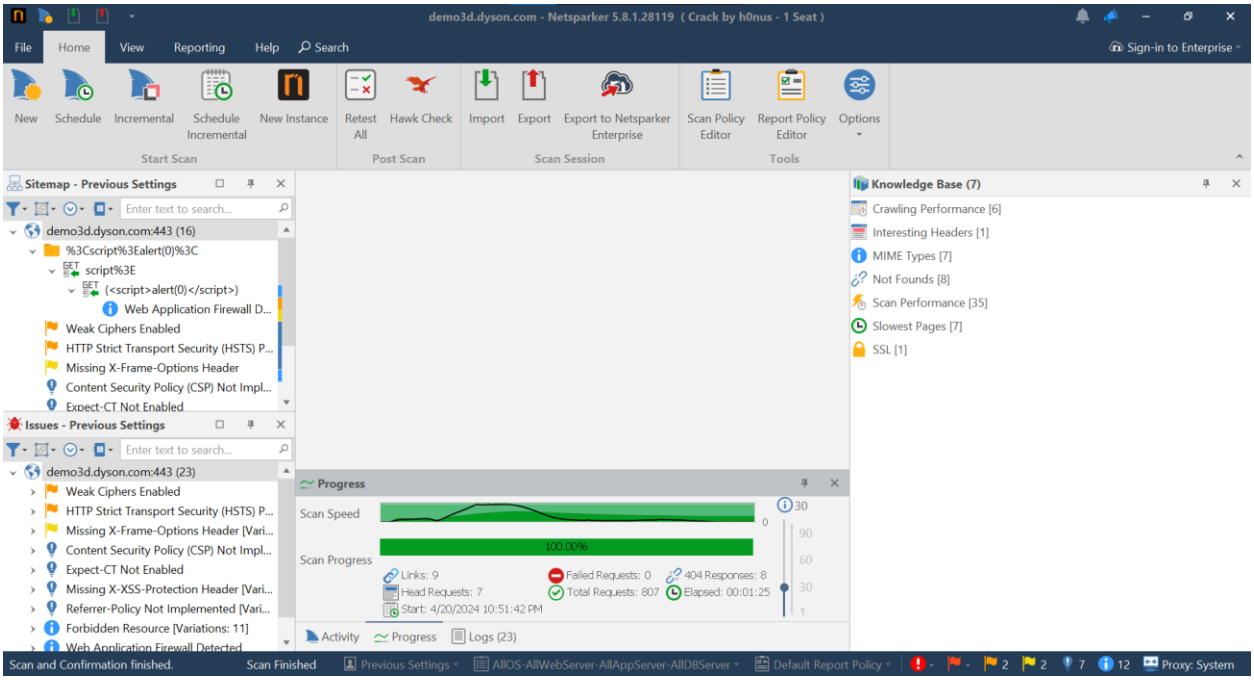
- **Nmap**

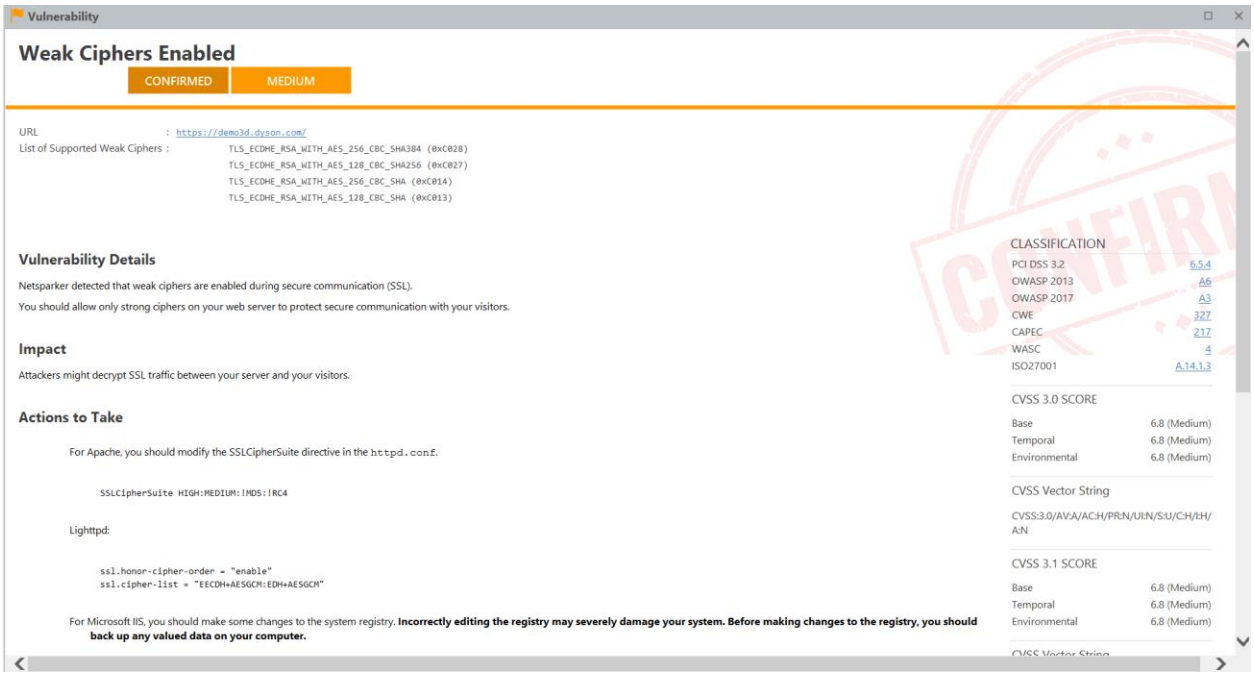
```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln demo3D.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 22:21 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
------------------ Timing report ------------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:21
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 22:22, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 22:22
mass_rdns: 0.15s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 22:22, 0.15s elapsed
DNS resolution of 1 IPs took 0.15s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 22:22
Scanning demo3D.dyson.com (184.50.85.169) [1000 ports]
Discovered open port 80/tcp on 184.50.85.169
Discovered open port 443/tcp on 184.50.85.169
Completed Connect Scan at 22:22, 6.08s elapsed (1000 total ports)
Overall sending rates: 329.34 packets / s.
NSE: Script scanning 184.50.85.169.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:22
NSE: Starting http-vuln-cve2013-0156 against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-vmware-path-vuln against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-vuln-cve2017-1001000 against demo3D.dyson.com (184.50.85.169:80).
NSE: Starting http-passwd against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-vuln-wnr1000-creds against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-vuln-cve2014-3704 against demo3D.dyson.com (184.50.85.169:80).
NSE: [http-vuln-cve2014-3704 184.50.85.169:80] adding admin user (username: 'lggorssvew'; passwd: 'olfdtbexse')
NSE: Starting http-stored-xss against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-iis-webdav-vuln against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-awstatstotals-exec against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-enum against demo3D.dyson.com (184.50.85.169:80).
NSE: [http-enum 184.50.85.169:80] Loading fingerprint database: /usr/bin/../share/nmap/nselib/data/http-fingerprints.lua
NSE: [http-enum 184.50.85.169:80] Loaded 299 fingerprints
NSE: Starting http-csrf against demo3D.dyson.com (184.50.85.169:443).
NSE: Starting http-shellshock against demo3D.dyson.com (184.50.85.169:443).
```

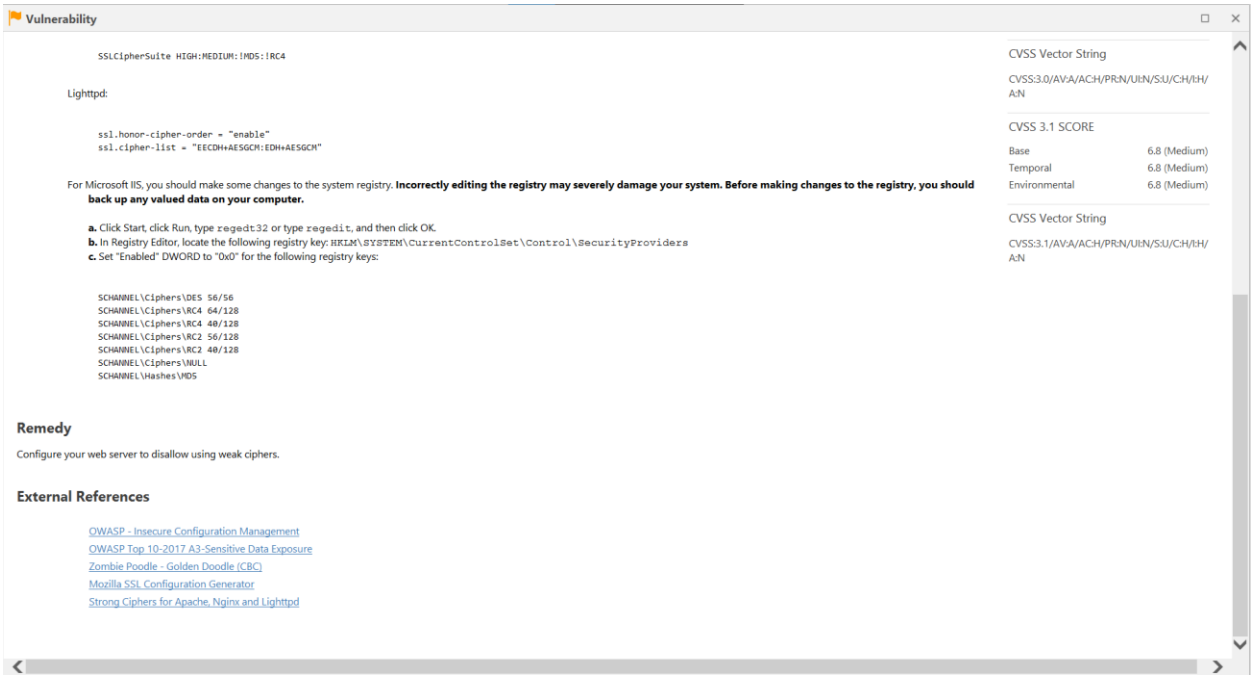
```
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  https   syn-ack
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
| http-vuln-cve2014-2129:
|_  ERROR: Not a Cisco ASA or unsupported version
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2014-2127:
|_  ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2128:
|_  ERROR: Not a Cisco ASA or unsupported version
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2014-2126:
|_  ERROR: Not a Cisco ASA or unsupported version
Final times for host: srtt: 49935 rttvar: 16177  to: 114643
```

Zero vulnerabilities found

- **Netsparker**.


demo3d.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Retest All
Hawk Check
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Post Scan
Scan Session
Tools
Sitemap - Previous Settings
demo3d.dyson.com:443 (16)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Issues - Previous Settings
demo3d.dyson.com:443 (23)
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header [Vari...
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Missing X-XSS-Protection Header [Vari...
Referrer-Policy Not Implemented [Vari...
Forbidden Resource [Variations: 11]
Web Application Firewall Detected
Progress
Scan Speed
Scan Progress
100.00%
Links: 9
Head Requests: 7
Start: 4/20/2024 10:51:42 PM
Failed Requests: 0
Total Requests: 807
404 Responses: 8
Elapsed: 00:01:25
Activity
Progress
Logs (23)
Knowledge Base (7)
Crawling Performance [6]
Interesting Headers [1]
MIME Types [7]
Not Founds [8]
Scan Performance [35]
Slowest Pages [7]
SSL [1]
Scan and Confirmation finished.
Scan Finished
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy
Proxy: System


Vulnerability
Weak Ciphers Enabled
CONFIRMED
MEDIUM
URL : https://demo3d.dyson.com/
List of Supported Weak Ciphers :
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
Vulnerability Details
Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Impact
Attackers might decrypt SSL traffic between your server and your visitors.
Actions to Take
For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
Lighttpd:
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
For Microsoft IIS, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.
CLASSIFICATION
PCI DSS 3.2 6.5.4
OWASP 2013 A6
OWASP 2017 A3
CWE 327
CAPEC 217
WASC 4
ISO27001 A.14.1.3
CVSS 3.0 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)
CVSS Vector String
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
CVSS 3.1 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)



Vulnerability

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

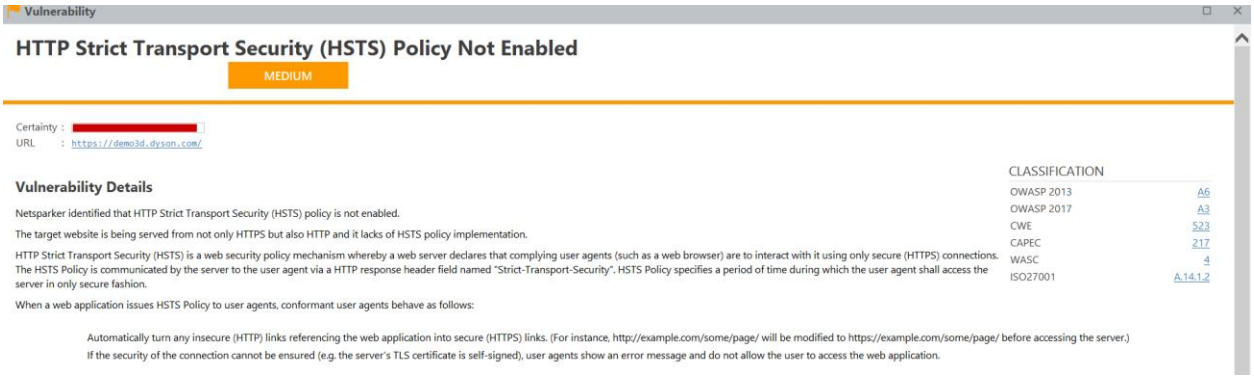
CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

addressing this vulnerability by disallowing the use of weak ciphers is crucial for enhancing the security of SSL communication and mitigating the risk of decryption attacks by malicious actors.



Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :
URL : https://demo3d.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Vulnerability

server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
      ServerAlias *
      RewriteEngine On
      RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
     # Use HTTP Strict Transport Security to force client to use secure connections only
     Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

     # Further Configuration goes here
     [...]
</VirtualHost>
```

External References

Wikipedia - HTTP Strict Transport Security
Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
HTTP Strict Transport Security (HSTS) HTTP Header
Mozilla SSL Configuration Generator

Addressing this vulnerability by implementing HSTS policy and redirecting HTTP traffic to HTTPS is crucial for enhancing the seurity of web communication and mitigating the risk of various attacks.

Vulnerability

Missing X-Frame-Options Header

LOW

Certainty :
URL : https://demo3d.dyson.com/

Vulnerability Details

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

`X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
`X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
`X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

Addressing this vulnerability by implementing the appropriate X-Frame-Options header is crucial for mitigating the risk of clickjacking attacks and enhancing the overall security of the website.

Report 09

Target sub domain : admin.shop.kr.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h admin.shop.kr.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.32.29.11, 96.17.180.45
+ Target IP:          23.32.29.11
+ Target Hostname:    admin.shop.kr.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 22:41:10 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; desc="1713408005315_387980551_124030596_29_8116_42_0_-";dur=1,).
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://admin.shop.kr.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8214 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-04-17 22:56:47 (GMT-4) (937 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on these findings there are a few vulnerabilities and security concerns to address

- The absence of the X-Frame-Options header leaves the site susceptible to clickjacking attacks.
- The lack of the X-Content-Type-Options header could lead to MIME type sniffing attacks.
- The presence of an uncommon header ('server-timing') may warrant further investigation to ensure it's not indicative of any security issues

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u http://admin.shop.kr.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ====
This scan has been saved in the file /home/rasan/.wapiti/scans/admin.shop.kr.dyson.com_folder_9aa7b5b0.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
OK
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
OK
Checking Strict-Transport-Security :
OK

[*] Launching module cookieflags
Checking cookie : AzureAppProxyPreauthSessionCookie_24ddf8d2-b5fb-4b59-a2ec-b2032feb06ec_60da6293-92b9-4a1e-ba93-1e09a01c578c_1.4
HttpOnly flag is not set in the cookie : AzureAppProxyPreauthSessionCookie_24ddf8d2-b5fb-4b59-a2ec-b2032feb06ec_60da6293-92b9-4a1e-ba93-1e09a01c578c_1.4
Checking cookie : AzureAppProxyAnalyticCookie_24ddf8d2-b5fb-4b59-a2ec-b2032feb06ec_https_1.3
HttpOnly flag is not set in the cookie : AzureAppProxyAnalyticCookie_24ddf8d2-b5fb-4b59-a2ec-b2032feb06ec_https_1.3
Checking cookie : buid
Checking cookie : fpc
Checking cookie : x-ms-gateway-slice
HttpOnly flag is not set in the cookie : x-ms-gateway-slice
Checking cookie : stsservicecookie
HttpOnly flag is not set in the cookie : stsservicecookie
Checking cookie : esctx
Checking cookie : esctx=mPtR95JyAtg
Checking cookie : esctx=sEbZ6I6qYlc

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss
```

Wapiti vulnerability report

Target: http://admin.shop.kr.dyson.com/

Date of the scan: Thu, 18 Apr 2024 02:42:49 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	1
HttpOnly Flag cookie	4
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-XSS-Protection is not set
```

Solutions

Use the recommendations for hardening your HTTP Security Headers.

References

- Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications
- KeyCDN: Hardening Your HTTP Security Headers
- OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)

HttpOnly Flag cookie

Description

HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie (if the browser supports it).

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : AzureAppProxyPreauthSessionCookie_24ddf8d2-b5fb-4b59-a2ec-b2032feb
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : AzureAppProxyAnalyticCookie_24ddf8d2-b5fb-4b59-a2ec-b2032feb06ec_h
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : x-ms-gateway-slice
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
HttpOnly flag is not set in the cookie : stsservicecookie
```

Solutions

While creation of the cookie, make sure to set the HttpOnly Flag to True.

References

- OWASP: Testing for Cookies Attributes
- OWASP: HttpOnly

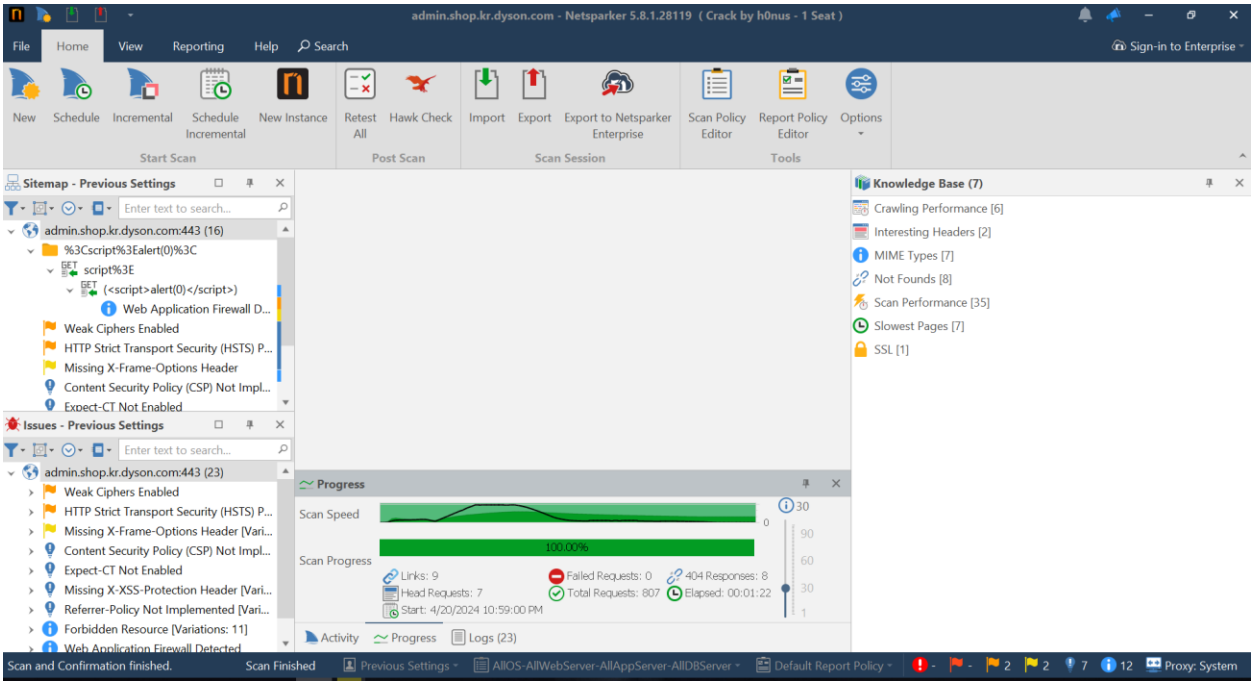
- **Whatweb**

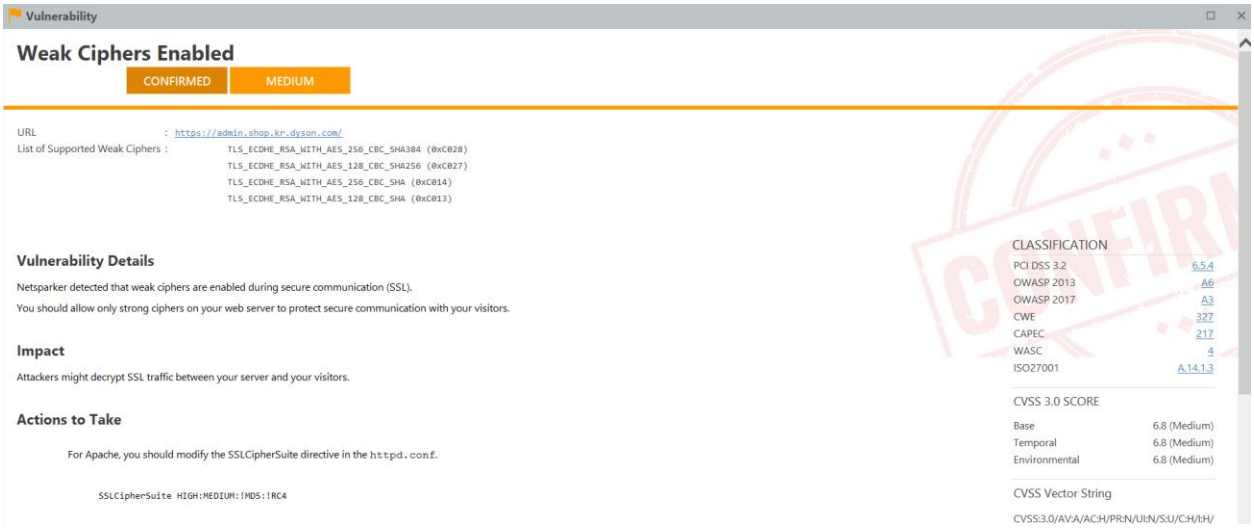
```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 admin.shop.kr.dyson.com
WhatWeb report for http://admin.shop.kr.dyson.com
Status    : 403 Forbidden
Title     : Access Denied
IP        : 23.32.29.11
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost], UncommonHeaders[server-timing]

Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website     : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String      : AkamaiGHost (from server string)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String      : server-timing (from headers)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 381
        Expires: Thu, 18 Apr 2024 02:47:12 GMT
        Cache-Control: max-age=0, no-cache, no-store
        Pragma: no-cache
        Date: Thu, 18 Apr 2024 02:47:12 GMT
        Connection: close
        Server-Timing: cdn-cache; desc=HIT
        Server-Timing: edge; dur=1
        Server-Timing: ak_p; desc="1713408432096_387980551_127665828_15_4326_200_0_-";dur=1
```

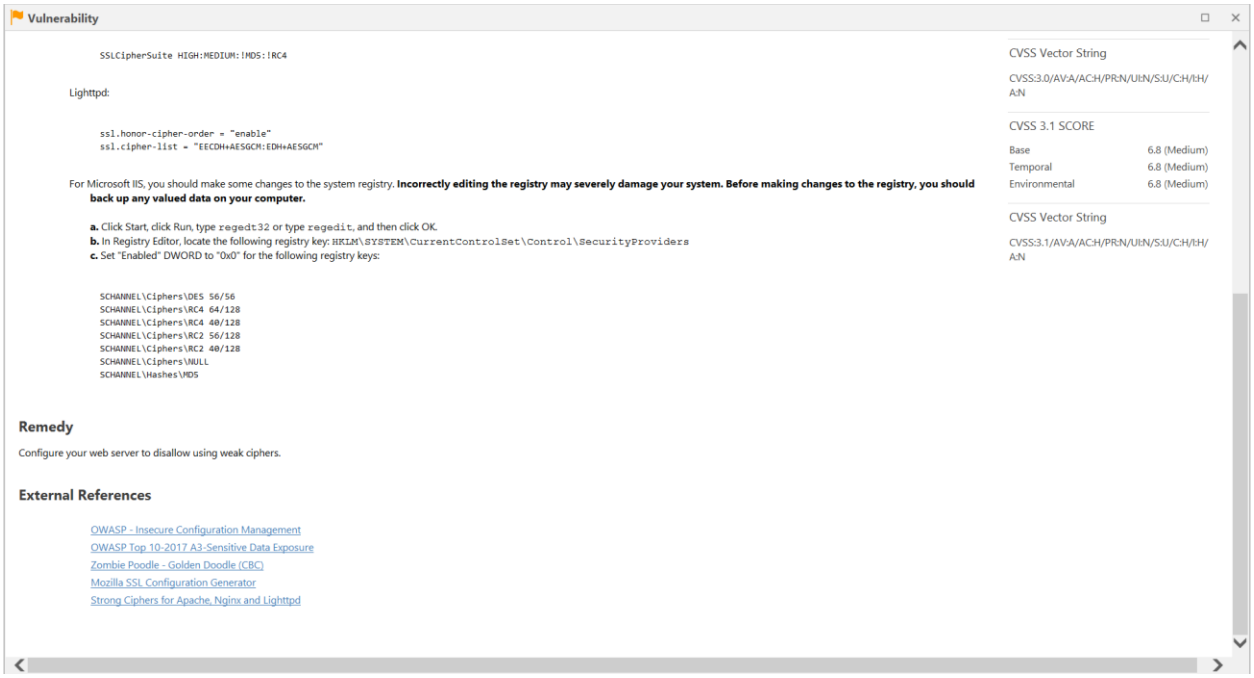
- **Nmap**

```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln admin.shop.kr.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 22:41 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
NSOCK INFO [0.0s] nsock_iod_new2(): nsock_iod_new(IOD #1)
NSOCK INFO [0.0s] nsock_write(): IOD #1 WRITE (127.0.0.1:53) [28]
```

- **Netsparker**


admin.shop.kr.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Retest All
Hawk Check
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Post Scan
Scan Session
Tools
Sitemap - Previous Settings
admin.shop.kr.dyson.com:443 (16)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Issues - Previous Settings
admin.shop.kr.dyson.com:443 (23)
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header [Vari...
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Missing X-XSS-Protection Header [Vari...
Referrer-Policy Not Implemented [Vari...
Forbidden Resource [Variations: 11]
Web Application Firewall Detected
Knowledge Base (7)
Crawling Performance [6]
Interesting Headers [2]
MIME Types [7]
Not Founds [8]
Scan Performance [35]
Slowest Pages [7]
SSL [1]
Progress
Scan Speed
Scan Progress
100.00%
Links: 9
Head Requests: 7
Start: 4/20/2024 10:59:00 PM
Failed Requests: 0
Total Requests: 807
404 Responses: 8
Elapsed: 00:01:22
Activity
Progress
Logs (23)
Scan and Confirmation finished.
Scan Finished
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy
Proxy: System


Vulnerability
Weak Ciphers Enabled
CONFIRMED
MEDIUM
URL : https://admin.shop.kr.dyson.com/
List of Supported Weak Ciphers : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
Vulnerability Details
Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Impact
Attackers might decrypt SSL traffic between your server and your visitors.
Actions to Take
For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
CLASSIFICATION
PCI DSS 3.2 6.5.4
OWASP 2013 A6
OWASP 2017 A3
CWE 327
CAPEC 217
WASC 4
ISO27001 A.14.1.3
CVSS 3.0 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)
CVSS Vector String
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/



Vulnerability

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Addressing this vulnerability by disallowing the use of weak ciphers is crucial for protecting the confidentiality and integrity of data transmitted over SSL, thus enhancing the overall security posture of the website.

Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :

URL : https://admin.shop.kr.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
```

Vulnerability

server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

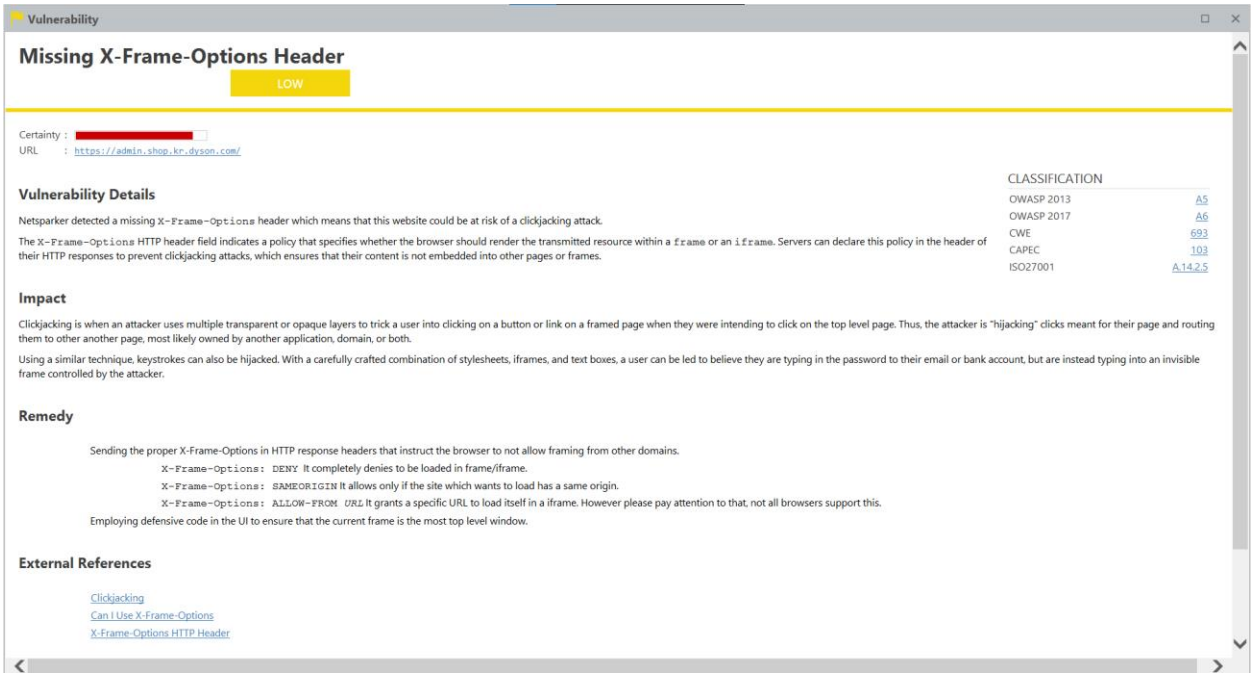
i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

Wikipedia - HTTP Strict Transport Security
Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
HTTP Strict Transport Security (HSTS) HTTP Header
Mozilla SSL Configuration Generator

Implementing an HSTS policy is essential for ensuring secure communication between the server and user agents, thereby mitigating the risk of potential security vulnerabilities associated with unsecured HTTP connections.



Vulnerability

Missing X-Frame-Options Header

LOW

Certainty :

URL : https://admin.shop.kr.dyson.com/

Vulnerability Details

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.

X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.

X-Frame-Options: ALLOW-FROM *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

Clickjacking

Can I Use X-Frame-Options

X-Frame-Options HTTP Header

implementing the X-Frame-Options header with the appropriate settings is essential for mitigating the risk of clickjacking attacks and enhancing the security of the website.

Report 10

Target sub domain : staging.admin.shop.kr.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h staging.admin.shop.kr.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 184.28.235.43, 184.28.235.75, 64:ff9b::b81c:eb2b, 64:ff9b::b81c:eb4b
+ Target IP:          184.28.235.43
+ Target Hostname:    staging.admin.shop.kr.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 23:25:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; desc="1713410640694_3088902951_467259632_44_14098_257_0_-";dur=1,).
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://staging.admin.shop.kr.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
^[[A^[[A^[[A^[[A^[[A^[[A+ 8301 requests: 2 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-04-18 00:02:51 (GMT-4) (2267 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on these findings there are a few vulnerabilities and security concerns to address

- The absence of the X-Frame-Options header leaves the site susceptible to clickjacking attacks.
- The lack of the X-Content-Type-Options header could lead to MIME type sniffing attacks.
- The presence of an uncommon header ('server-timing') may warrant further investigation to ensure it's not indicative of any security issues.

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u https://staging.admin.shop.kr.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ----
This scan has been saved in the file /home/rasan/.wapiti/scans/staging.admin.shop.kr.dyson.com_folder_4ce96f08.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=yjfb2r for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
------
A report has been generated in the file /home/rasan/.wapiti/generated_report
Open /home/rasan/.wapiti/generated_report/staging.admin.shop.kr.dyson.com_04182024_0401.html with a browser to see this report.
```

Wapiti vulnerability report

Target: https://staging.admin.shop.kr.dyson.com/

Date of the scan: Thu, 18 Apr 2024 04:01:10 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Frame-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-XSS-Protection is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Content-Type-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
Strict-Transport-Security is not set
```

Solutions

Use the recommendations for hardening your HTTP Security Headers.

References

- Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications
- KeyCDN: Hardening Your HTTP Security Headers
- OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)

Wapiti 3.0.4 © Nicolas SURRIBAS 2006-2021

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 staging.admin.shop.kr.dyson.com
WhatWeb report for http://staging.admin.shop.kr.dyson.com
Status    : 403 Forbidden
Title     : Access Denied
IP        : 23.215.7.26
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost], UncommonHeaders[server-timing]

Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website     : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : AkamaiGHost (from server string)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : server-timing (from headers)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 397
        Expires: Thu, 18 Apr 2024 04:04:37 GMT
        Date: Thu, 18 Apr 2024 04:04:37 GMT
        Connection: close
        Server-Timing: cdn-cache; desc=HIT
        Server-Timing: edge; dur=1
        Server-Timing: ak_p; desc="1713413077318_389065882_440483910_12_5478_240_0_-";dur=1
```

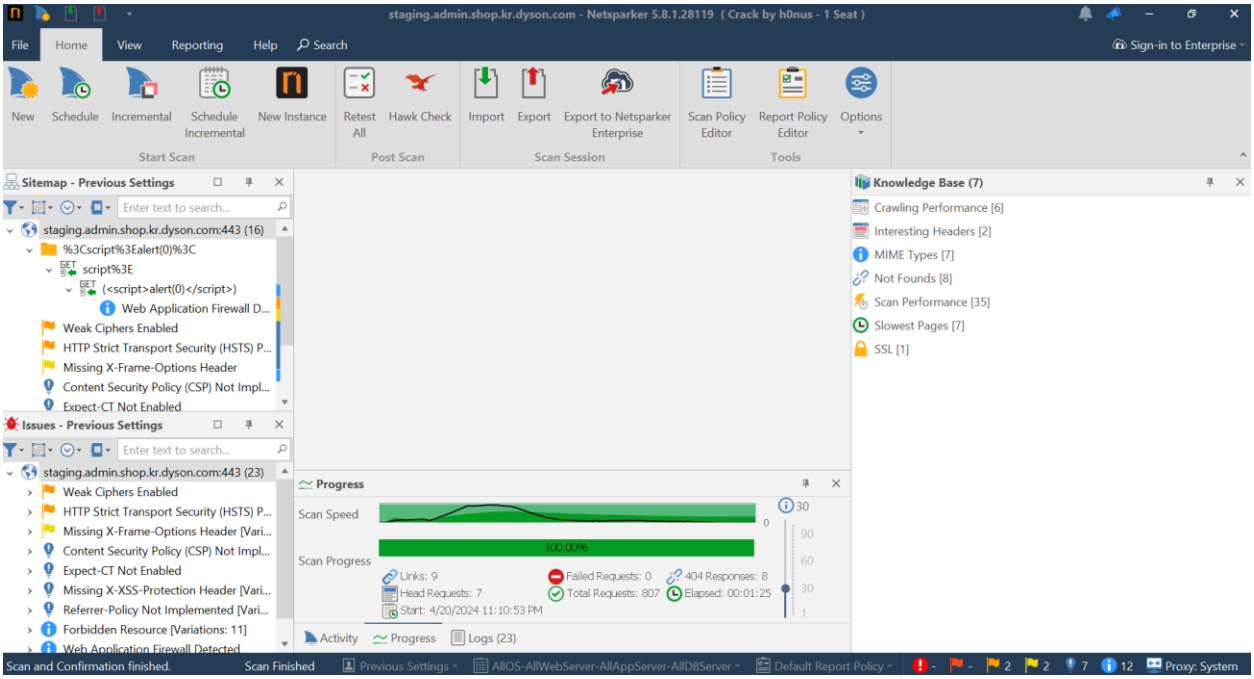
- **Nmap**

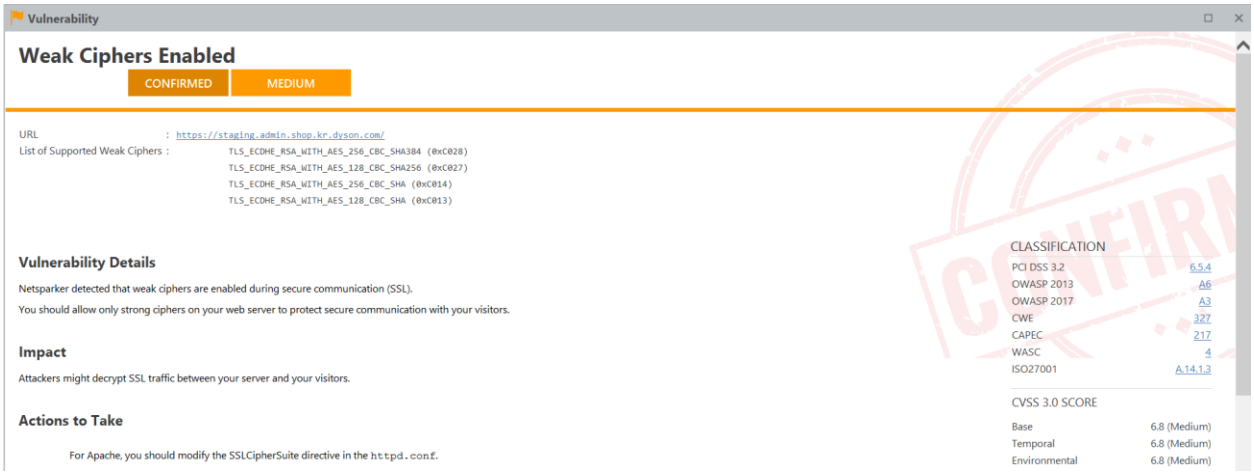
```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln staging.admin.shop.kr.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 23:26 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
------------------ Timing report ------------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:26
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 23:26, 10.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:26
Completed NSE at 23:26, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 23:26
mass_rdns: 0.05s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 23:26, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 23:26
Scanning staging.admin.shop.kr.dyson.com (23.209.46.133) [1000 ports]
Discovered open port 25/tcp on 23.209.46.133
Discovered open port 443/tcp on 23.209.46.133
Discovered open port 80/tcp on 23.209.46.133
Completed Connect Scan at 23:26, 6.40s elapsed (1000 total ports)
Overall sending rates: 312.51 packets / s.
NSE: Script scanning 23.209.46.133.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:26
NSE: Starting http-shellshock against staging.admin.shop.kr.dyson.com (23.209.46.133:80).
NSE: [http-shellshock 23.209.46.133:80] Sending '() { :;}; echo; echo -n xqcztrk; echo lnghdpr' in HTTP headers:User-Agent,Cookie and Referer
NSE: Starting http-dlink-backdoor against staging.admin.shop.kr.dyson.com (23.209.46.133:80).
NSE: Starting http-stored-xss against staging.admin.shop.kr.dyson.com (23.209.46.133:80).
NSE: Starting ssl-known-key against staging.admin.shop.kr.dyson.com (23.209.46.133:443).
NSE: Starting http-vmware-path-vuln against staging.admin.shop.kr.dyson.com (23.209.46.133:443).
NSE: Starting http-sql-injection against staging.admin.shop.kr.dyson.com (23.209.46.133:443).
NSE: [firewall-bypass] lacks privileges.
NSE: Starting http-vuln-cve2014-8877 against staging.admin.shop.kr.dyson.com (23.209.46.133:443).
NSE: Starting http-shellshock against staging.admin.shop.kr.dyson.com (23.209.46.133:443).
NSE: [http-shellshock 23.209.46.133:443] Sending '() { :;}; echo; echo -n ioyzrys; echo ijewplz' in HTTP headers:User-Agent,Cookie and Referer
NSE: Starting http-vuln-cve2013-7091 against staging.admin.shop.kr.dyson.com (23.209.46.133:443).
NSE: [http-vuln-cve2013-7091 23.209.46.133:443] Trying to detect if the server is vulnerable
NSE: [http-vuln-cve2013-7091 23.209.46.133:443] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../dev/null%00
```

```
PORT     STATE SERVICE REASON
25/tcp   open  smtp    syn-ack
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
80/tcp   open  http    syn-ack
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp  open  https   syn-ack
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
Final times for host: srtt: 18521 rttvar: 15220  to: 100000
```

Zero vulnerabilities found.

- **Netsparker**


staging.admin.shop.kr.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Retest All
Hawk Check
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Post Scan
Scan Session
Tools
Sitemap - Previous Settings
staging.admin.shop.kr.dyson.com:443 (16)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Issues - Previous Settings
staging.admin.shop.kr.dyson.com:443 (23)
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header [Vari...
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Missing X-XSS-Protection Header [Vari...
Referrer-Policy Not Implemented [Vari...
Forbidden Resource [Variations: 11]
Web Application Firewall Detected
Knowledge Base (7)
Crawling Performance [6]
Interesting Headers [2]
MIME Types [7]
Not Founds [8]
Scan Performance [35]
Slowest Pages [7]
SSL [1]
Progress
Scan Speed
Scan Progress
100.00%
Links: 9
Head Requests: 7
Start: 4/20/2024 11:10:53 PM
Failed Requests: 0
Total Requests: 807
404 Responses: 8
Elapsed: 00:01:25
Activity
Progress
Logs (23)
Scan and Confirmation finished.
Scan Finished
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy
Proxy: System


Vulnerability
Weak Ciphers Enabled
CONFIRMED
MEDIUM
URL : https://staging.admin.shop.kr.dyson.com/
List of Supported Weak Ciphers :
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
Vulnerability Details
Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Impact
Attackers might decrypt SSL traffic between your server and your visitors.
Actions to Take
For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
CLASSIFICATION
PCI DSS 3.2 6.5.4
OWASP 2013 A6
OWASP 2017 A3
CWE 327
CAPEC 217
WASC 4
ISO27001 A.14.1.3
CVSS 3.0 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)

Vulnerability

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

It's crucial to address this vulnerability by configuring the web server to only allow strong ciphers thereby enhancing the security of SSL communication and reducing the risk of data compromise.

Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty : [redacted]
URL : https://staging.admin.shop.kr.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
```

Vulnerability

server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

Wikipedia - HTTP Strict Transport Security
Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
HTTP Strict Transport Security (HSTS) HTTP Header
Mozilla SSL Configuration Generator

it's crucial to address this vulnerability by implementing HSTS to ensure that all communication with the website occurs over secure HTTPS connections thereby mitigating the risk of certain types of attacks and enhancing overall security.

Vulnerability

Missing X-Frame-Options Header

LOW

Certainty :

URL : https://staging.admin.shop.kr.dyson.com/

Vulnerability Details

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

`X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.

`X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.

`X-Frame-Options: ALLOW-FROM URL` It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

Clickjacking

Can I Use X-Frame-Options

X-Frame-Options HTTP Header

It is important to address this vulnerability by implementing the X-Frame-Options header to protect against potential clickjacking attacks and enhance the security of the website.

Report 11

Target sub domain : privacy.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h privacy.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.215.7.27, 23.215.7.16
+ Target IP:          23.215.7.27
+ Target Hostname:    privacy.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-17 23:25:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: Cookie _abck created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie bm_sz created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; desc="1713410663347_389065883_338056750_14_11911_70_0_-";dur=1,).
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://privacy.dyson.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'AkamaiGHost' to 'Microsoft-IIS/10.0'.
+ /webservices/IlaWebServices: Uncommon header 'x-correlation' found, with contents: 38624645-76b7-4bb3-9013-f7a3051ea098.
+ 8050 requests: 1 error(s) and 7 item(s) reported on remote host
+ End Time:           2024-04-18 00:01:15 (GMT-4) (2148 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on these findings there are several vulnerabilities and security concerns to address

- Cookies created without the httponly flag could be vulnerable to client-side attacks.
- The absence of the X-Frame-Options header leaves the site susceptible to clickjacking attacks.
- The lack of the X-Content-Type-Options header could lead to MIME type sniffing attacks.
- The presence of uncommon headers may warrant further investigation to ensure they're not indicative of any security issues.

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u http://privacy.dyson.com/

   __  __                _ _   _ _____
   / / /\ \ \__ _ _ __ (_)_(_)___ /
   \ \/  \/ / _` | '_ \| | | __|| |_ \
    \  /\  / (_| | |_) | | |_| |___) |
     \/  \/ \__,_| .__/|_|\__|_|____/
                 |_|
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Resuming scan from previous session, please wait
[*] Saving scan state, please wait ...

 Note
 ========
This scan has been saved in the file /home/rasan/.wapiti/scans/privacy.dyson.com_folder_52de9eae.db
[*] Wapiti found 15 URLs and forms during the scan
[*] Loading modules:
         backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, x

[*] Launching module csp
CSP attribute "default-src" is missing
CSP attribute "script-src" is missing
CSP attribute "object-src" is missing
CSP attribute "base-uri" is missing

[*] Launching module http_headers
Checking X-Frame-Options :
OK
Checking X-XSS-Protection :
OK
Checking X-Content-Type-Options :
OK
Checking Strict-Transport-Security :
OK

[*] Launching module cookieflags
Checking cookie : _abck
HttpOnly flag is not set in the cookie : _abck
Secure flag is not set in the cookie : _abck
```

- **Whatweb**

```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 privacy.dyson.com
WhatWeb report for http://privacy.dyson.com
Status    : 403 Forbidden
Title     : Access Denied
IP        : 23.215.7.16
Country   : UNITED STATES, US

Summary   : Akamai-Global-Host, HTTPServer[AkamaiGHost], UncommonHeaders[server-timing]

Detected Plugins:
[ Akamai-Global-Host ]
        Akamai-Global-Host HTTPd

        Website     : https://www.akamai.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.
        String       : AkamaiGHost (from server string)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : server-timing (from headers)

HTTP Headers:
        HTTP/1.1 403 Forbidden
        Server: AkamaiGHost
        Mime-Version: 1.0
        Content-Type: text/html
        Content-Length: 371
        Expires: Thu, 18 Apr 2024 04:31:02 GMT
        Date: Thu, 18 Apr 2024 04:31:02 GMT
        Connection: close
        Server-Timing: cdn-cache; desc=HIT
        Server-Timing: edge; dur=1
        Server-Timing: ak_p; desc="1713414662397_389065883_368787490_22_6593_0_0_-";dur=1
```

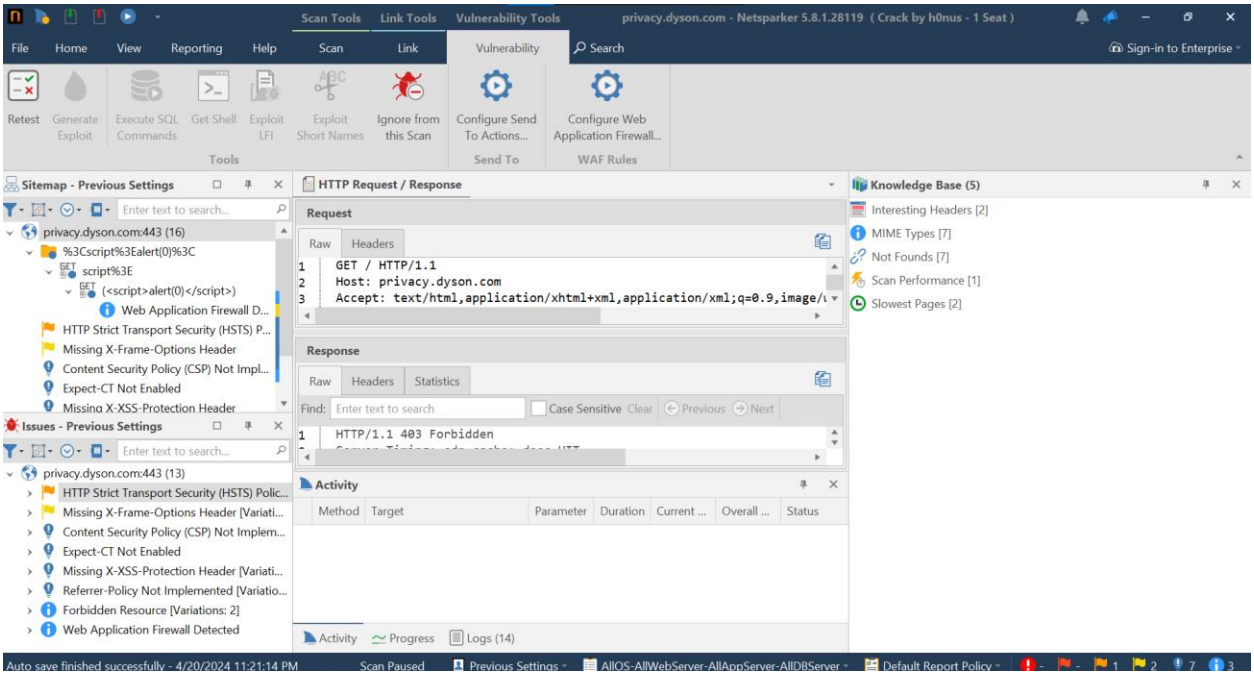
- **Nmap**

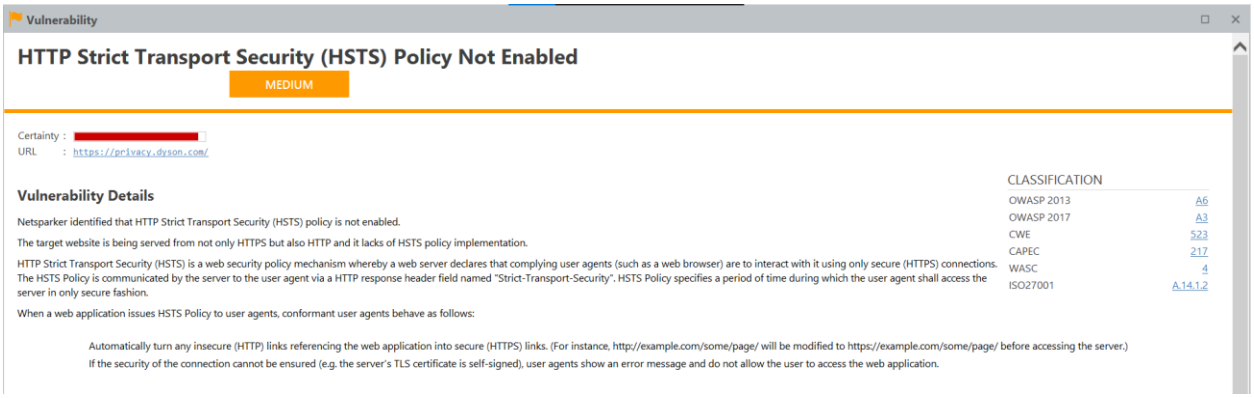
```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln privacy.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 23:59 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
                    ---------- Timing report ----------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:59
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 23:59, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:59
Completed NSE at 23:59, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 23:59
mass_rdns: 0.96s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 23:59, 0.96s elapsed
DNS resolution of 1 IPs took 0.96s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 23:59
Scanning privacy.dyson.com (23.215.7.27) [1000 ports]
Discovered open port 80/tcp on 23.215.7.27
Discovered open port 443/tcp on 23.215.7.27
Discovered open port 25/tcp on 23.215.7.27
Increasing send delay for 23.215.7.27 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Completed Connect Scan at 00:00, 44.83s elapsed (1000 total ports)
Overall sending rates: 45.19 packets / s.
NSE: Script scanning 23.215.7.27.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:00
NSE: Starting http-dlink-backdoor against privacy.dyson.com (23.215.7.27:443).
NSE: Starting http-vuln-cve2010-0738 against privacy.dyson.com (23.215.7.27:443).
NSE: [tls-ticketbleed] Not running due to lack of privileges.
NSE: Starting http-method-tamper against privacy.dyson.com (23.215.7.27:443).
NSE: Starting http-vuln-cve2013-7091 against privacy.dyson.com (23.215.7.27:80).
NSE: [http-vuln-cve2013-7091 23.215.7.27:80] Trying to detect if the server is vulnerable
NSE: [http-vuln-cve2013-7091 23.215.7.27:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../dev/null%00
NSE: [http-vuln-cve2013-7091 23.215.7.27:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../etc/passwd%00
NSE: Starting http-internal-ip-disclosure against privacy.dyson.com (23.215.7.27:80).
NSE: Starting http-vuln-cve2014-2129 against privacy.dyson.com (23.215.7.27:443).
NSE: Starting http-dombased-xss against privacy.dyson.com (23.215.7.27:443).
NSE: Starting http-vuln-cve2013-6786 against privacy.dyson.com (23.215.7.27:443).
NSE: Starting http-huawei-hg5xx-vuln against privacy.dyson.com (23.215.7.27:80).
```

```
PORT     STATE SERVICE REASON
25/tcp   open  smtp    syn-ack
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
80/tcp   open  http    syn-ack
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
443/tcp open  https   syn-ack
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
|_http-dombased-xss: Couldn't find any DOM based XSS.
Final times for host: srtt: 45695 rttvar: 6627  to: 100000

NSE: Script Post-scanning.
```

Zero vulnerabilities found.

- **Netsparker**


Scan Tools
Link Tools
Vulnerability Tools
privacy.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Scan
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Sitemap - Previous Settings
HTTP Request / Response
Knowledge Base (5)
Interesting Headers [2]
MIME Types [7]
Not Founds [7]
Scan Performance [1]
Slowest Pages [2]
privacy.dyson.com:443 (16)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
HTTP Strict Transport Security (HSTS) P...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Missing X-XSS-Protection Header
Request
Raw
Headers
GET / HTTP/1.1
Host: privacy.dyson.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Response
Raw
Headers
Statistics
HTTP/1.1 403 Forbidden
Issues - Previous Settings
privacy.dyson.com:443 (13)
HTTP Strict Transport Security (HSTS) Polic...
Missing X-Frame-Options Header [Variati...
Content Security Policy (CSP) Not Implem...
Expect-CT Not Enabled
Missing X-XSS-Protection Header [Variati...
Referrer-Policy Not Implemented [Variatio...
Forbidden Resource [Variations: 2]
Web Application Firewall Detected
Activity
Method
Target
Parameter
Duration
Current ...
Overall ...
Status
Activity
Progress
Logs (14)
Auto save finished successfully - 4/20/2024 11:21:14 PM
Scan Paused
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy


Vulnerability
HTTP Strict Transport Security (HSTS) Policy Not Enabled
MEDIUM
Certainty :
URL : https://privacy.dyson.com/
Vulnerability Details
Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.
The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.
When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:
Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.
CLASSIFICATION
OWASP 2013 A6
OWASP 2017 A3
CWE 523
CAPEC 217
WASC 4
ISO27001 A.14.1.2

Vulnerability

server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
      ServerAlias *
      RewriteEngine On
      RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
     # Use HTTP Strict Transport Security to force client to use secure connections only
     Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

     # Further Configuration goes here
     [...]
</VirtualHost>
```

External References

Wikipedia - HTTP Strict Transport Security
Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
HTTP Strict Transport Security (HSTS) HTTP Header
Mozilla SSL Configuration Generator

It is crucial to address this vulnerability by enabling HSTS policy to ensure that all interactions with the website occur over secure HTTPS connections thereby enhancing the overall security posture of the site.

Vulnerability

Missing X-Frame-Options Header

LOW

Certainty :
URL : https://privacy.dyson.com/

Vulnerability Details

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

`X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
`X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
`X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

Clickjacking
Can I Use X-Frame-Options
X-Frame-Options HTTP Header

Addressing this vulnerability by implementing the X-Frame-Options header with an appropriate directive will help prevent clickjacking attacks and enhance the overall security of the website.

Report 12

Target sub domain : teamcenterMY.dyson.com

- **Nikto**

```
┌──(rasan㉿kali)-[~]
└─$ nikto -h teamcenterMY.dyson.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 20.199.104.59, 64:ff9b::14c7:683b
+ Target IP:          20.199.104.59
+ Target Hostname:    teamcenterMY.dyson.com
+ Target Port:        80
+ Start Time:         2024-04-18 00:14:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8046 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2024-04-18 00:42:51 (GMT-4) (1699 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Based on these findings there are a couple of vulnerabilities and security concerns to address

- The absence of the X-Frame-Options header leaves the site susceptible to clickjacking attacks.
- The lack of the X-Content-Type-Options header could lead to MIME type sniffing attacks.

- **Wapiti**

```
┌──(rasan㉿kali)-[~]
└─$ wapiti -u https://teamcenterMY.dyson.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Resuming scan from previous session, please wait
[*] Saving scan state, please wait ...

 Note
 ----
This scan has been saved in the file /home/rasan/.wapiti/scans/teamcenterMY.dyson.com_folder_465754dc.db
[*] Wapiti found 3 URLs and forms during the scan
[*] Loading modules:
       backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=m1nsau for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
------
```

Wapiti vulnerability report

Target: https://teamcenterMY.dyson.com/

Date of the scan: Thu, 18 Apr 2024 04:34:33 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	2
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	8
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Frame-Options is not set
```

Vulnerability found in /

Description HTTP Request cURL command line

```
X-XSS-Protection is not set
```

Vulnerability found in /

Description HTTP Request cURL command line

```
X-Content-Type-Options is not set
```

Vulnerability found in /

Description HTTP Request cURL command line

```
Strict-Transport-Security is not set
```

Vulnerability found in /

Description HTTP Request cURL command line

```
X-Frame-Options is not set
```

Vulnerability found in /

Description HTTP Request cURL command line

```
X-XSS-Protection is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Content-Type-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
Strict-Transport-Security is not set
```

Solutions

Use the recommendations for hardening your HTTP Security Headers.

References

- Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications
- KeyCDN: Hardening Your HTTP Security Headers
- OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)

Wapiti 3.0.4 © Nicolas SURRIBAS 2006-2021

- **Whatweb**

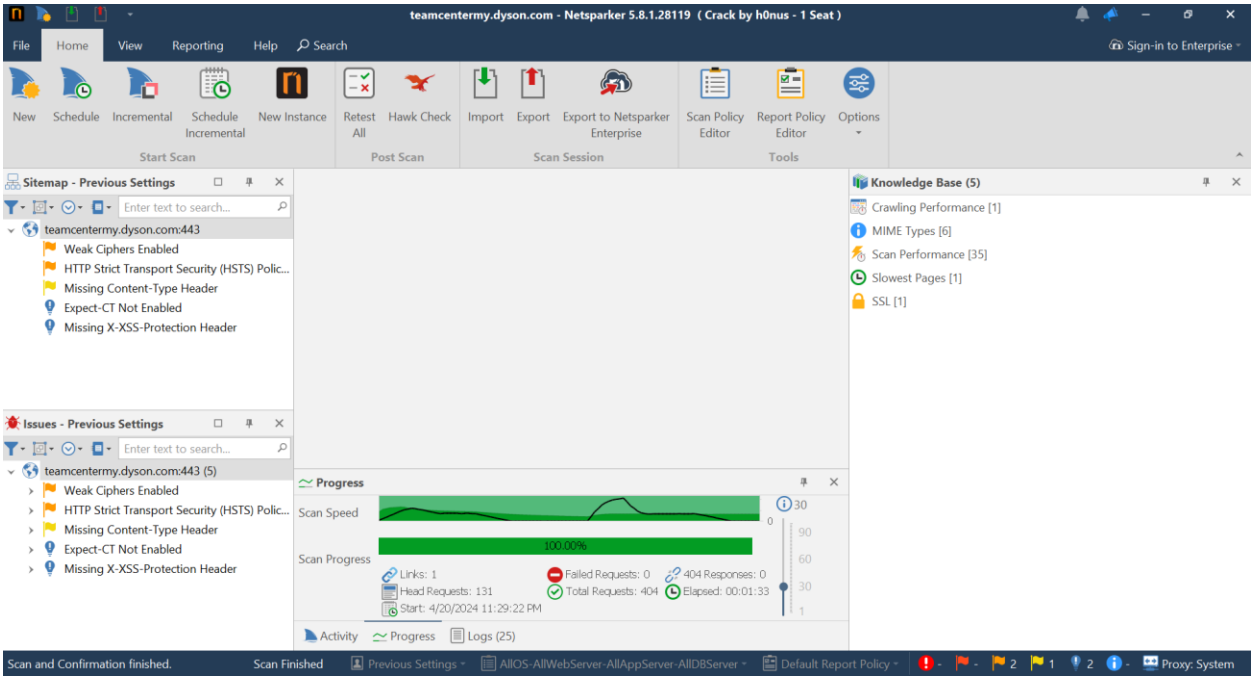
```
┌──(rasan㉿kali)-[~]
└─$ whatweb -v -a 1 teamcenterMY.dyson.com
WhatWeb report for http://teamcenterMY.dyson.com
Status    : 404 Not Found
Title     : <None>
IP        : 20.199.104.59
Country   : UNITED STATES, US

Summary   :

Detected Plugins:
HTTP Headers:
        HTTP/1.1 404 Not Found
        Transfer-Encoding: chunked
        Date: Thu, 18 Apr 2024 04:38:50 GMT
        Connection: close
```

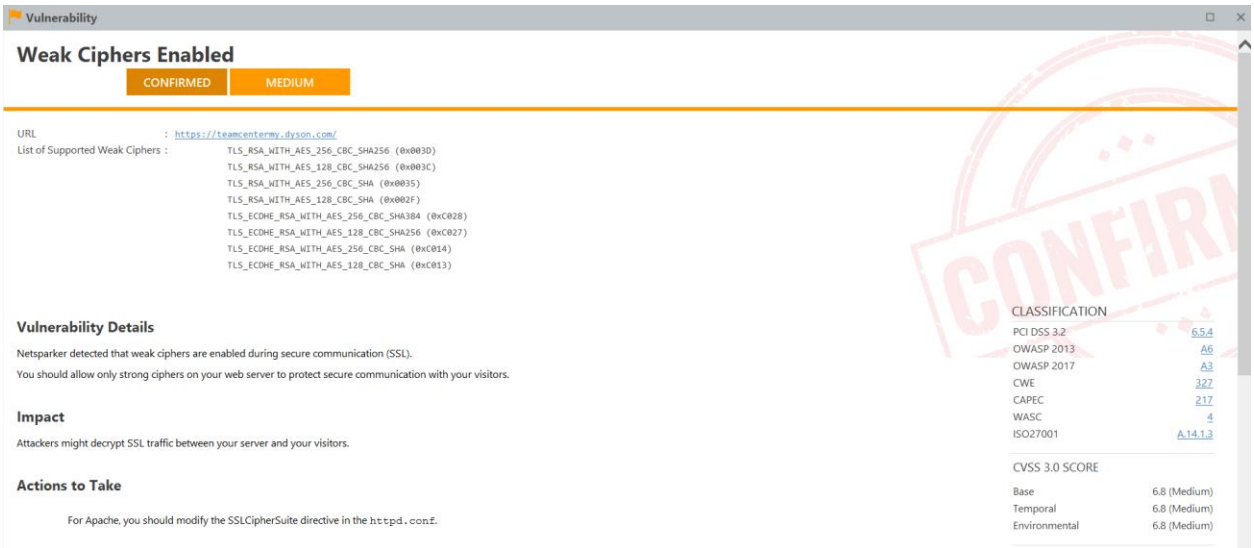
- **Nmap**

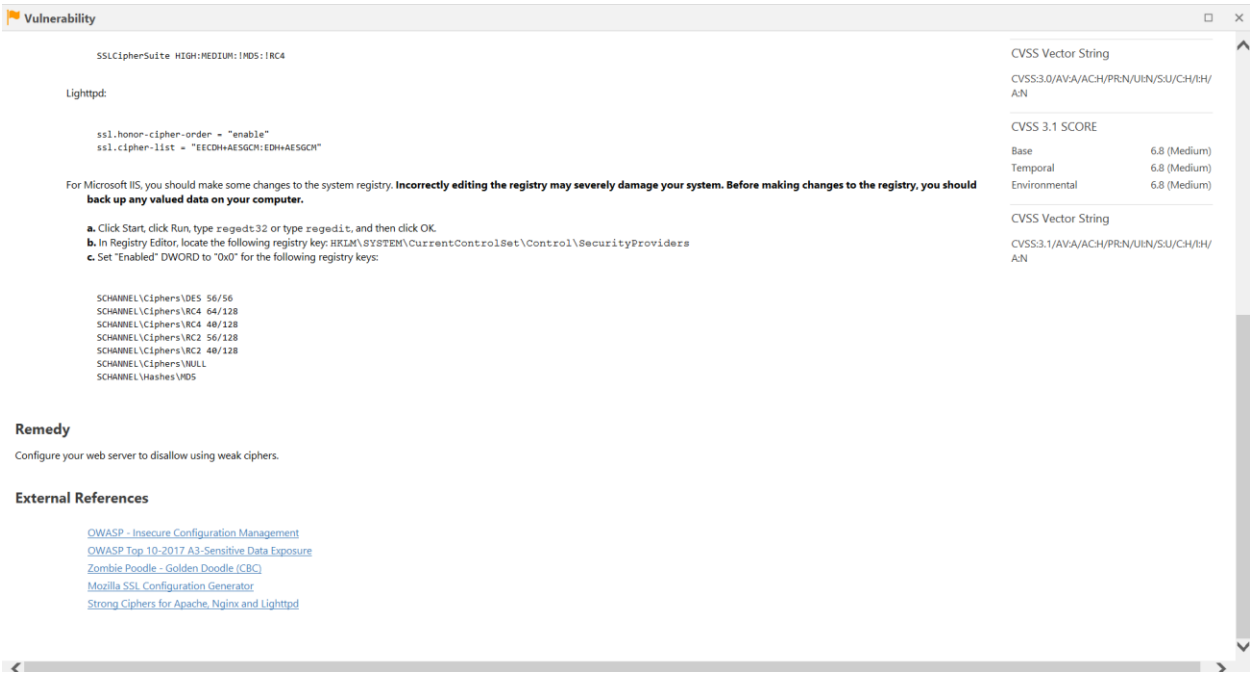
```
┌──(rasan㉿kali)-[~]
└─$ nmap -Pn -d --script vuln teamcenterMY.dyson.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-18 00:28 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
------------------ Timing report ------------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:28
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 00:29, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:29
Completed NSE at 00:29, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 00:29
mass_rdns: 0.23s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 00:29, 0.23s elapsed
DNS resolution of 1 IPs took 0.23s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 00:29
Scanning teamcenterMY.dyson.com (20.199.104.59) [1000 ports]
Discovered open port 443/tcp on 20.199.104.59
Discovered open port 80/tcp on 20.199.104.59
Completed Connect Scan at 00:29, 13.67s elapsed (1000 total ports)
Overall sending rates: 146.65 packets / s.
NSE: Script scanning 20.199.104.59.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:29
NSE: Starting http-passwd against teamcenterMY.dyson.com (20.199.104.59:443).
NSE: Starting http-fileupload-exploiter against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: Starting http-frontpage-login against teamcenterMY.dyson.com (20.199.104.59:443).
NSE: Starting http-vuln-cve2017-8917 against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: [http-vuln-cve2017-8917 20.199.104.59:80] Attacking uri /index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1,concat(1,user()),1)
NSE: Starting http-vmware-path-vuln against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: Starting http-vuln-cve2014-8877 against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: Starting http-vuln-cve2014-2126 against teamcenterMY.dyson.com (20.199.104.59:443).
NSE: Starting http-vuln-misfortune-cookie against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: Starting http-vuln-cve2010-0738 against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: Starting http-awstatstotals-exec against teamcenterMY.dyson.com (20.199.104.59:443).
NSE: Starting http-frontpage-login against teamcenterMY.dyson.com (20.199.104.59:80).
NSE: Starting http-tplink-dir-traversal against teamcenterMY.dyson.com (20.199.104.59:443).
NSE: [http-tplink-dir-traversal 20.199.104.59:443] HTTP GET /help/../../etc/shadow
NSE: Starting http-trace against teamcenterMY.dyson.com (20.199.104.59:80).
```

```
PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-iis-webdav-vuln:
|_  ERROR: This web server is not supported.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
443/tcp open  https   syn-ack
| http-iis-webdav-vuln:
|_  ERROR: This web server is not supported.
| http-vuln-cve2014-2127:
|_  ERROR: Failed to connect to SSL VPN server
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2014-2126:
|_  ERROR: Failed to connect to SSL VPN server
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-vuln-cve2014-2129:
|_  ERROR: Failed to connect to SSL VPN server
| http-vuln-cve2014-2128:
|_  ERROR: Failed to connect to SSL VPN server
Final times for host: srtt: 179500 rttvar: 30394  to: 301076
```

- **Netsparker**


teamcentermy.dyson.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Retest All
Hawk Check
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Post Scan
Scan Session
Tools
Sitemap - Previous Settings
Enter text to search...
teamcentermy.dyson.com:443
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) Polic...
Missing Content-Type Header
Expect-CT Not Enabled
Missing X-XSS-Protection Header
Knowledge Base (5)
Crawling Performance [1]
MIME Types [6]
Scan Performance [35]
Slowest Pages [1]
SSL [1]
Issues - Previous Settings
teamcentermy.dyson.com:443 (5)
Progress
Scan Speed
Scan Progress
100.00%
Links: 1
Head Requests: 131
Start: 4/20/2024 11:29:22 PM
Failed Requests: 0
Total Requests: 404
404 Responses: 0
Elapsed: 00:01:33
Activity
Progress
Logs (25)
Scan and Confirmation finished.
Scan Finished
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy
Proxy: System


Vulnerability
Weak Ciphers Enabled
CONFIRMED
MEDIUM
URL : https://teamcentermy.dyson.com/
List of Supported Weak Ciphers :
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
Vulnerability Details
Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Impact
Attackers might decrypt SSL traffic between your server and your visitors.
Actions to Take
For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
CLASSIFICATION
PCI DSS 3.2 6.5.4
OWASP 2013 A6
OWASP 2017 A3
CWE 327
CAPEC 217
WASC 4
ISO27001 A.14.1.3
CVSS 3.0 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)



Vulnerability

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management
OWASP Top 10-2017 A3-Sensitive Data Exposure
Zombie Poodle - Golden Doodle (CBC)
Mozilla SSL Configuration Generator
Strong Ciphers for Apache, Nginx and Lighttpd

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

addressing this vulnerability by disallowing weak ciphers will help protect the secure communication between the server and visitors there by enhancing the overall security of the website.

Vulnerability

HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :

URL : https://teamcentermy.dyson.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
```

Vulnerability

server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

Wikipedia - HTTP Strict Transport Security
Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
HTTP Strict Transport Security (HSTS) HTTP Header
Mozilla SSL Configuration Generator

enabling HSTS policy and redirecting HTTP traffic to HTTPS will help mitigate the security risks associated with insecure connections and enhance the overall security posture of the website.